

INTERVIEWING TO ASSESS AND MANAGE THREATS OF VIOLENCE

Renate Geurts

Defended 1 September 2017

Revised submission 20 October 2017

The thesis is submitted in partial fulfilment of the requirements for the award of the degree of Doctor of Philosophy of the University of Portsmouth.

This work was funded by the Erasmus Mundus Joint Doctoral program in Legal Psychology (EMJD-LP) under Framework Partnership Agreement (FPA) 2013-0036 and Specific Grant Agreement (SGA) 2014-0678.

Supervised by Professor Aldert Vrij, Dr Samantha Mann, and Dr Sharon Leal.

GENERAL ABSTRACT

Geurts, R. (2017). *Interviewing to Assess and Manage Threats of Violence*. Department of Psychology, University of Portsmouth.

Persons who pose threats of violence can be rich sources of information for professionals charged with ensuring safety and security. The interviewing of threateners is thus considered important among such professionals, but research on the topic is scarce. This thesis seeks to advance current knowledge by proposing a scientific perspective on effective threat assessment and management (TAM) interviewing. What are the expected dynamics when interacting with persons who threaten to cause harm and, given these dynamics, which interview methods work best? A novel experimental paradigm was developed and employed in Studies I, II, and III. Participants were given a fictitious case describing two conflicting parties and were then asked to take on the role of the threatening party in a subsequent interview with the conflicting party. **Study I** ($N = 157$) examined whether individuals' intent to actualise a threat becomes evident in how they verbalise that threat. Intent was manipulated across three conditions through the likelihood to actualise the threat: low likelihood (no intent: *bluffers*), medium likelihood (weak intent: *conditional actualisers*), and high likelihood (strong intent: *decisive actualisers*). Based on theory and research in cognitive psychology, it was predicted that decisive actualisers would provide the most detail about the implementation of the threat, followed by conditional actualisers, and bluffers would provide the least. The opposite trend was found: Persons more likely to actualise a threat were found to be less informative about its implementation. **Study II** ($N = 179$) tested the effect of two interview techniques (*low* vs. *high suspicion-oriented*) on the information provided by bluffers and actualisers. Drawing on psychological research examining lie detection, it was theorised that the need to be believed would be more urgent for bluffers than for actualisers. Hence, bluffers were expected to be more forthcoming when questioned about their threats and, in particular, when the questions communicated suspicion. As expected, bluffers provided more information in response to specific questions as compared to actualisers, especially with regard to implementation details (replicating Study I). However, the difference between bluffers and actualisers was not further accentuated by the use of suspicion-oriented questions. Furthermore, Study II explored whether threatening participants had used counter-interview strategies. Participants were found to be forthcoming, while also being strategic and adaptive to interviewers' responses. **Study III** ($N = 120$) tested the hypothesis that *rapport-based interviewing* would be more effective for threat assessment and management purposes than *direct interviewing*. Against expectations, no differences were

found between interview protocols pertaining to the threateners' use of counter-interview strategies, their information provision, or their willingness to pursue/discuss the threat. Furthermore, the study advanced Study II by exploring what types of counter-interview strategies threateners employ. Again, threateners were found to be both forthcoming and strategic. The most frequently reported strategies were to *prove capability* and to *conceal information*. **Study IV** was an online study that investigated whether threat assessments made by professionals were of higher quality than those made by non-professionals. Threat assessment professionals, university students, and laypersons assessed the risk for violence in three fictitious cases. In alignment with the literature on expert decision-making, it was predicted that professionals (vs. students and laypersons) would agree more with one another with respect to risk assessments and that their information search would more resemble empirically supported threat cues. The results supported both hypotheses. Taking the results of the studies together, it could be concluded that threateners are semi-cooperative interviewees, whose attitudes may not be impacted by general interview approaches (e.g. *rapport-based*, *suspicion-oriented*). Instead, the findings suggest that more strategic techniques developed from the perspective of threateners (which result in their motivation to be informative prevailing over their need to be strategic) are needed.

Key words: threat assessment, threat management, investigative interviewing, true and false intent, human intelligence gathering

TABLE OF CONTENTS

Declaration	ii
List of Figures and Tables	iii
Abbreviations	iv
Acknowledgements	v
Dissemination	vii
 Chapter 1: General Introduction	 1
Defining Threats and the Scope of the Thesis	3
Research and Practice in Threat Assessment and Management	4
Research on True and False Intentions	11
Research on Human Intelligence Interviewing	14
A Novel Experimental Paradigm	19
 Chapter 2: Summary of Empirical Studies	 22
Study I	23
Study II	30
Study III	43
Study IV	51
 Chapter 3: General Discussion	 63
Main Findings	63
Limitations	69
Future Research	70
Ethical Considerations	73
Conclusions	74
 References	 76
 Appendices	 90

Appendix A: Favourable Ethical Opinion (Study I & Study II)	89
Appendix B: Favourable Ethical Opinion (Study III)	90
Appendix C: Favourable Ethical Opinion (Study IV)	91
Appendix D: UPR16 Form	92
Appendix E: Manuscript Study I	94
Appendix F: Manuscript Study II	106
Appendix G: Manuscript Study III	115
Appendix H: Manuscript Study IV	143

DECLARATION

Whilst registered as a candidate for the above degree, I have not been registered for any other research award. The results and conclusions embodied in this thesis are the work of the named candidate and have not been submitted for any other academic award.

A handwritten signature in purple ink, appearing to read 'Renate Geurts', with a large, stylized initial 'R' and a horizontal line extending from the end of the name.

Renate Geurts

WORD COUNT = 33.254 words (excluding appendices)

LIST OF FIGURES AND TABLES

Figure 1a	Total amount of information provided by bluffers and actualisers in the free-statement phase and in the specific-questions phase (Study II)	39
Figure 1b	Amount of ‘why’ and ‘how’ information provided by bluffers and actualisers (Study II)	39
Figure 2	Risk assessments (1 = <i>very strong risk decrease</i> , 9 = <i>very strong risk increase</i>) that professionals, students, and laypersons made for the information cues presented per case (Study IV)	57
Table 1	Overview of Studies Constituting this Thesis	22
Table 2	Descriptive Statistics for the Amount (Top Panel) and Timing (Bottom Panel) of ‘Why’ and ‘How’ Information Revealed by Bluffers, Conditional Actualisers, and Decisive Actualisers (Study I)	28
Table 3	Interview Protocols That Were Used to Answer the Participants’ Threat Calls (Study II)	33
Table 4	Mean Values (and Standard Deviations) of Bluffers’ and Actualisers’ Involvement with the Case, Experienced Difficulty to Comply with the Instructions, and Nervousness about Performing the Tasks (Study II)	36
Table 5	Mean values (and Standard Deviations) for the Amount of Information that Bluffers and Actualiser Provided in their Threat Statements by Phase, Protocol, and Information (Study II)	38
Table 6	Reported Strategies by Bluffers and Actualisers (Study II)	40
Table 7	Frequencies of Threateners’ Self-Reported Counter-Interview Strategies (Study III)	47
Table 8	Means of Before- and After-Interview Ratings as a Function of Interview Protocol (Study III)	48
Table 9	Areas of Inquiry Used to Classify Requested Information (Study IV)	55
Table 10	Mean Percentages for Violence Risk per Case Judged by Professionals, Students, and Laypersons (Study IV)	58
Table 11	Means and Inferential Statistics for the Analyses of the Requested Information (Study IV)	60

ABBREVIATIONS

AETAP	: Association of European Threat Assessment Professional
ATAP	: Association of Threat Assessment Professional
CATAP	: Canadian Association of Threat Assessment Professional
CLT	: Construal Level Theory
CTAP-25	: Communications Threat Assessment Protocol-25
ECSP	: Exceptional Case Study Project
FTAC	: Fixated Threat Assessment Centre
HUMINT	: Human Intelligence
NCAVC	: National Centre for the Analysis of Violent Crimes
NGO	: Non-Governmental Organisation
PCL-R	: Psychopathy Checklist-Revised
PEACE	: Planning and preparation, Engage and explain, Account, Closure, Evaluation
SARA	: Spousal Assault Risk Assessment Guide
SJP	: Structural Professional Judgment
SUE	: Strategic Use of Evidence
TAM	: Threat Assessment and Management
TRAP-18	: Terrorist Radicalisation Assessment Protocol-18
WAVR-21	: Workplace Assessment of Targeted Violence Risk-21

ACKNOWLEDGMENTS

Thank you to my supervisors who have contributed most to the completion of this dissertation. Professor *Pär Anders Granhag*, you have guided me through these years with great charm and integrity. I have secretly wished you could be my supervisor forever. Putting foolish wishes aside, I'm just grateful and proud to have learned from you. Associate Professor *Karl Ask*, you seem to excel at everything you do. Your talent would have intimidated me if not for your kindness. Thank you for motivating me with intellect and care. Professor *Aldert Vrij*, you are faster than the spell checker when reviewing my manuscripts. I appreciate your speed, explicitness, and sympathy.

Thanks to the great number of people who assisted in data collection, translations, and coding. This thesis is built on your endurance. Thanks also to Dr. *Samantha Mann* and Dr. *Sharon Leal*, for providing valuable feedback to this thesis. A special thanks to the opponents, Professor *Ellen Giebels* and Dr. *Ryan Fitzgerald*, for sharing your wisdom with me.

To my friends and colleagues in the Department of Psychology, you have been, by far, the best part of my work. Never in my life have I drunk so much coffee but you were worth the new addiction. To all members of the research unit for Criminal, Legal, and Investigative Psychology (CLIP), I now understand what it means to work in an inspiring environment and it has been my privilege. To *Erik* and *Elaine*, on whom I have relied zillion times, you comfort me and make me laugh. Thank you for your friendship.

I have no hobbies and I don't play sports, but I do have friends and I cannot think of a better way to spend my time. Leaving you behind has been the biggest challenge of my PhD abroad. *Julie, Charlotte, Kim, Gina, Marthe, Myrthe, Merel, Liesbeth, Sara, Natasha, Judy* and *Helene*, you have warmed my heart with endless visits to Gothenburg and Portsmouth. Thank you.

Thank you to *Agneta, Gabriella, Johan, Adolf*, and *Kristin*, for making me feel part of a family when mine was far away.

One cannot choose family, but if I could, I would have chosen mine. To my brothers, *Remco, Bruno*, and *Lucas*, your existence is as special as it is natural to me. To my sisters-in-law, *Eva* and *Jutta*, thank you for warming my home with your company. To my nephews, *Krijn* and *Piet*, loving you is effortless.

To my parents, *Joost* and *Marie-Claire*, to whom I owe most, if not all, I have. You have secured me with love and support. I now feel grounded among anyone. Anywhere. At any time. Thank you infinitely.

Dear *Simon*, it is amazing how little else I need when you are with me. Thank you for loving me so loyally and unpretentiously. You are my dearest memory of Sweden and I'm grateful to call this the start.

Renate Geurts
Gothenburg, July 2017

DISSEMINATION

Conference Presentations

- Geurts, R., Granhag, P. A., Ask, K., & Vrij, A. (2014, November). *Separating threats from bluffs: A research outline*. Oral presentation at the Nordic Network for Psychology & Law (NNPL), Oslo, Norway.
- Geurts, R., Granhag, P. A., Ask, K., & Vrij, A. (2015, August). *Identifying markers of true threats*. Poster presentation at the European Association of Psychology and Law (EAPL), Nuremberg, Germany.
- Geurts, R., Granhag, P. A., Ask, K., & Vrij, A. (2017, June). *Assessing threats of violence: Professional skill or common sense?* Oral presentation at the European Association of Psychology and Law (EAPL), Mechelen, Belgium.

Seminar Presentations

- Geurts, R., Granhag, P. A., Ask, K., & Vrij, A. (2016, November). *Assessing threats of violence*. Oral Presentation at Iowa State University, Ames, US.
- Geurts, R., Granhag, P. A., Ask, K., & Vrij, A. (2016, December). *Assessing threats of violence*. Oral Presentation at a research seminar with the Norwegian Police Academy, Gothenburg, Sweden.
- Geurts, R., Granhag, P. A., Ask, K., & Vrij, A. (2016, August). *Threat Assessment*. Oral Presentation at a research seminar with the Centre for Ethics, Law, and Mental Health (CELAM), Gothenburg, Sweden.

Publications

- Geurts, R., Granhag, P. A., Ask, K., & Vrij, A. (2016). Taking threats to the lab: Introducing an experimental paradigm for studying verbal threats. *Journal of Threat Assessment and Management*, 3, 53-64. doi: 10.1037/tam0000060 [Study I]
- Geurts, R., Ask, K., Granhag, P. A., & Vrij, A. (2017). Eliciting information from people who pose a threat: Counter-interview strategies examined. *Journal of Applied Research in Memory and Cognition*, 6, 158-166. doi: 10.1016/j.jarmac.2016.10.002 [Study II]
- Geurts, R., Ask, K., Granhag, P. A., & Vrij, A. (2017). *Interviewing to manage threats: exploring the effects of interview style on information gain and threateners' counter-interview strategies*. Manuscript submitted for publication. [Study III]
- Geurts, R., Granhag, P. A., Ask, K., & Vrij, A. (2017). Assessing threats of violence: Professional skill or common sense? *Journal of Investigative Psychology and Offender Profiling*. Advanced online publication. doi: 10.1002/jip.1486 [Study IV]

CHAPTER 1: GENERAL INTRODUCTION

The *Journal of Threat Assessment and Management* recently published a special edition looking back at 25 years of research and practice in threat assessment and management (Guy, 2015). Professionals in this field are concerned with assessing and managing persons believed to pose a threat of violence (Meloy, 2015). With a history of less than three decades, the field is still young. Modern threat assessment originated in law enforcement and intelligence agencies when, in the late eighties, the US Secret Service was challenged by the assassination of public officials. These incidents gave rise to one of the pioneering projects in threat assessment: the Exceptional Case Study Project (ECSP; Fein & Vossekuil, 1999). The ECSP examined 83 assassins of Secret Service protectees and the overall aim was to reach an understanding of the perpetrators' backgrounds, motives, and behaviours. The findings of this project resulted in the first operational guidelines on how to assess threats of violence (Fein & Vossekuil, 1998). Notably, the lessons learned then still prevail today (Borum, Fein, Vossekuil, & Berglund, 1999; Guy, 2015). These lessons were: (i) violence is presumed to result from understandable thoughts and behaviours, (ii) such thoughts and behaviours develop over time, (iii) they are shaped by experiences (rather than personality), and (iv) they are often evident in subjects' behaviour prior to an attack. Identifying such behaviours is considered key to threat assessment investigations.

Has nothing changed then over the past few decades? The answer is to the contrary; the field of threat assessment has developed rapidly. A number of archival studies followed the ECSP, which not only addressed violence towards public figures but also workplace violence, school violence, and domestic violence (mostly stalking). In addition to these domains, the 9/11 attacks in 2001 brought about studies examining radicalisation and terrorist intent. Knowledge development resulted in jargon and threat assessment tools, and it allowed for specialisation. Today, practitioners can join associations for threat assessment professionals, attend conferences, enrol in training courses, and apply for certification.

When reviewing 25 years of work, it becomes obvious that remarkable progress has been made. However, such a review also identifies knowledge gaps and obstacles. Critiques have been raised with regard to widely used terminology and concepts (Hart, 2016a). For instance, threat assessment is often defined as assessing the risk for *targeted violence*, which implies that there exists non-targeted violence as well — but how does that differ from an accident? Moreover, subjects of concern are assumed to move through sequential stages of a pathway towards violence, but how long does it take to move from one stage to another? Can

subjects move backwards or skip stages? What are the factors pushing an individual to the next stage? And are there pathways to non-violence too? In addition to conceptual ambiguities, methodological difficulties limit the field. One such difficulty is that the base rates of risk factors are largely unknown (Gill, 2015). To illustrate, if there is no grasp of how many people in society experience feelings of hopelessness, it is hard to say whether or not feelings of hopelessness are typical for the offender population (and thus indicative of risk). Finally, I would allow myself to add one more issue to the list of future challenges: How can valuable information be collected from persons who pose a threat of violence?

The person posing a threat is arguably the richest source of information for threat managers. However, such subjects are also the most difficult sources of information. They may exaggerate or downplay their intentions, they may conceal or lie about their plans, they may be unable to give a comprehensive account (potentially due to mental illness), or interviewing them might increase the risk for violence (Meloy, Hart, & Hoffmann, 2014a). These conditions emphasise the need for skilled interviewing. Although the importance of interviewing is acknowledged in the literature on threat assessment (Calhoun & Weston, 2015; Fein & Vossekuil, 1998; Mohandie, 2014; van der Meer & Diekhuis, 2014), there has been surprisingly little research on *how* to conduct such interviews. Threat assessment interviewers might rely on findings from related disciplines such as suspect interviewing and crisis negotiation, or they might draw on customary knowledge that has emerged over time through experience (Hartwig, Meissner, & Semel, 2014). However, given the developments in the field, a unique research strand is merited on interviewing to assess and manage threats of violence.

The central aim of this thesis is to contribute to a scientific approach for *threat assessment and management (TAM) interviewing*. Specifically, the thesis seeks to make such a contribution by: (i) reviewing relevant research and methodology in social, legal, and cognitive psychology, and thereby providing a theoretical groundwork for examining TAM interviews, (ii) introducing and testing an experimental paradigm for studying interview dynamics in TAM contexts, and (iii) reflecting on the outcomes of the empirical studies in order to identify future avenues for research. The content of the thesis is structured accordingly.

Defining Threats and the Scope of the Thesis

Definitions

Deep water, bad weather, political tension, and viral outbreaks — many insecurities can be threatening. However, these are not the types of threats examined in this thesis. Instead, the focus is on *threats of violence*. Violence can be defined as actual, attempted, or threatened physical or serious psychological harm that a person deliberately directs without consent towards another person(s) (e.g. Douglas et al., 2014). Note that this definition excludes suicidal threats. Moreover, according to this definition, all communicated threats should be considered violence, but not all violence involves threats. In addition, all harm that one threatens to inflict is violence as well. This can be physical, emotional, or financial harm, disturbance of peace, or persistent harassing behaviour.

Within threat assessment and management, the term “threat” can mean two things. The first meaning refers to an act that communicates an intent to cause violence—the person *makes* a threat. Persons who make a threat are, in this thesis, indicated as *threateners*, a term derived from the act of threatening. The second meaning describes a situation of potential violence. In these situations, there is concern that a specific person will act violently—the person *poses* a threat (Fein et al., 1995). A person who poses a threat is a subject of concern, yet not a threatener. The concepts of posing and making a threat relate to each other as follows. Persons can make an explicit threat without posing a threat (i.e. they are bluffing). Persons can pose a threat without making a threat (i.e. they have harmful intentions but remain silent). Lastly, persons can both make and pose a threat (i.e. they have harmful intentions and communicate them). These three groups form the bulk of worrisome cases that professionals must triage. Note that persons can move from one group to another over time and/or in different situations. For instance, a person who makes a threat might be bluffing at first but then decides to carry out the threat when their threat is ignored. Threat assessments can thus require altering quickly, which is why assessment is considered a dynamic process (Meloy et al., 2014a). For the empirical studies in this thesis, participants always made a threat that they either meant to actualise or not. In other words, subjects of concern who conceal their harmful intentions have not been studied here (see the General Discussion for an elaboration of this topic).

Further, the terms *threat assessment* and *threat management* are interdependent and often used interchangeably. However, they actually refer to different aspects of the same professional field. Threat assessment is the process of information gathering to understand and

evaluate a threat of violence, whereas threat management is the process of developing and executing plans to mitigate the threat of violence (Meloy et al., 2014a). Both terms are used throughout the thesis depending on the topic discussed.

Finally, this thesis examines threat assessment and management (TAM) interviewing. TAM interviewing is defined here as an *interaction* between a professional (e.g. law enforcement or health care officials) and a threatener. Typically, for the professional, the aim of this interaction is to collect information to assess the risk for violence or to recommend appropriate interventions, but the interaction can also be used to mitigate the risk for violence (e.g. reducing tension, building trust, reaching out). In line with this, the primary focus of the empirical studies has been on collecting information (Study I, II, IV) and a secondary focus has been on mitigating risk (Study III).

Research Questions

The current thesis rests on four broad assumptions. First, social and cognitive processes guide the behaviour of threateners when they engage with professionals about the threat they may pose. Second, such processes can be studied and understood by means of experimental research. Third, understanding the cognitions of threateners allows the interviewer to adapt his/her interaction techniques accordingly. Fourth, such adaptations aid threat assessment and management. These assumptions underpin the overriding research question of the thesis: How should persons who pose a threat be interviewed in order to assess and manage the risk for violence? The thesis builds on four empirical studies addressing direct and indirect aspects of this research question. Specifically, is it possible to detect verbal cues to deceit in threat statements (Study I)? Is it possible to interview strategically to elicit or enhance verbal cues to deceit in threat statements (Study II)? Which interview approach contributes most to information gathering and threat de-escalation (Study III)? How does professional experience contribute to the quality of threat assessments (Study IV)?

Research and Practice in Threat Assessment and Management

Two Strands of Research

Experimental research on threat assessment is scarce. There exist some studies on threats as mechanisms of social control in an unpredictable environment (e.g. how threats can be used to influence a target; how targets react to threats; Milburn & Watman, 1981). More

recently, Taylor and colleagues (2013) conducted an experiment in which they analysed language as a means to detect insider threats. However, most empirical work in the field of threat assessment falls within the following two strands of research: archival studies and efficacy studies. Both types of studies address the same question. That is, is it possible to identify factors (e.g. behaviours, background characteristics) that are indicative for the risk for violence? However, the two strands of research approach this question from different perspectives. In archival studies, shared behaviours and characteristics are identified among samples of similar perpetrators (“Twenty out of 30 attackers of American celebrities were found to be psychotic”). The findings from such research are used to develop risk assessment instruments. In efficacy studies, these instruments are evaluated in terms of reliability (e.g. “Do different raters reach similar conclusions when applying the instrument?”) and validity (e.g. “Does the instrument differentiate between offenders and non-offenders?”). Both strands of research are discussed below.

Archival studies. Archival studies in threat assessment have examined multiple domains of violence, such as public figure violence (e.g. Meloy et al., 2011), stalking (e.g. Rosenfeld & Harmon, 2002), terrorism (e.g. Corner & Gill, 2015), school shootings (O’Toole, 2009), and workplace violence (e.g. Kelleher, 1997). Within each of these domains, specific risk factors could be identified. For instance, it was found that many stalkers who assaulted their victims had first directly threatened them (Rosenfeld & Harmon, 2002), whereas most school shooters were found to have leaked their violent plans indirectly to a third party (e.g. friend, classmate) prior to the attack (O’Toole, 2009). Moreover, employment instability is considered a risk factor for workplace violence (Meloy, White, & Hart, 2013), but it has not been found to be particularly significant when considering public figure violence (Meloy et al., 2011). Instead, mental illness (primarily pathological fixation) appears as a critical factor among persons who threaten and attack public figures (Hoffmann, 2009; Mullen et al., 2009). Specifically, those who demonstrate a sense of grandiosity and self-entitlement were found to be more likely to harass celebrities (e.g. Dietz et al., 1991), politicians (e.g. Scalora et al., 2002), and royalty (e.g. James et al., 2009). When examining rates of mental illness among a sample of terrorists, high rates were found among terrorists acting alone (31.9%), but the number was almost 14 times lower among terrorists acting in groups (3.4%; Corner & Gill, 2015). These findings illustrate that risk factors can be more or less relevant within different domains of violence, and even within different subgroups of a specific domain of violence.

That said, many risk factors in threat assessment are not domain specific. Comparing checklists across domains, many of the same risk indicators become apparent (e.g. MacKenzie et al., 2009; Meloy et al., 2013). Examples of shared risk indicators are violent ideation, social isolation, mental illness (psychosis, depression), substance use, antisocial traits (narcissism, psychopathy), and a history of violence. More broadly, many risk factors in threat assessment resemble factors that are predictive of violence in general (Harris, Rice, & Quinsey, 1993) and of suicide (Hall, Platt, & Hall, 1999). This holds particularly true for factors that are historical (e.g. prior violence), clinical (e.g. mental illness), or social (e.g. support system).

Furthermore, it has been suggested that, regardless of the domain, problematic behaviours of threateners evolve to violence along a similar pathway (Calhoun & Weston, 2003; Fein et al., 1995). This pathway consists of consecutive stages of proximity to an attack, ranging from grievance and violent ideation to preparations and the final decision to strike. It has been theorised that each stage is characterised by “warning behaviours” (Meloy, Hoffmann, Guldemann, & James, 2012). These are acute and dynamic changes in behaviour that constitute evidence of accelerating risk (e.g. buying a weapon). Empirical support for a pathway to violence and for warning behaviours is mixed. Some behaviours have been consistently identified in archival studies (e.g. fixation, leakage), whereas others seem to be drawn from anecdotes and professionals’ experience (e.g. novel aggression, energy outburst, see Meloy, Hoffmann, Roshdi, Glaz-Ocik, & Guldemann, 2014b, for an overview). Moreover, little research has been conducted on the sequence of warning behaviours (Gill, 2015; Hart, 2016a). The pathway to violence is portrayed by a single, one-way, consecutive sequence, but this assumption has not yet been demonstrated.

Efficacy studies. Currently, the best validated threat assessment tools have been taken from the field of violence risk assessment. It would go beyond the scope of this thesis to discuss the predictive efficacy of violence risk assessment tools as this is a research domain of its own (for an overview, see Heilbrun, Yasuhara, & Shah, 2010). Yet, some efficacy matters are worth addressing as relates to threat assessment.

Threat managers typically make use of risk assessment instruments that fit the *structured professional judgment* (SPJ) model. The SPJ model relies on the discretion of the professionals, while providing structure to their judgments via empirically informed guidelines (Guy, Packer, & Warnken, 2012). SPJ tools detail risk factors for violence that have been identified by a literature review and these tools can be seen as a memory aid or recommendation for the professional who needs to assess and manage risks for violence. Examples of SPJ tools

are the *Historical, Clinical, Risk management-20* (HCR-20; Douglas et al., 2014) and the *Sexual Violence Risk-20* (SVR-20; Boer, Hart, Kropp, & Webster, 1997) used to assess the risk for general violence and sexual violence, respectively. A meta-analytic evaluation of the SPJ model revealed good levels of predictive accuracy and, hence, supported the utility of the model in assessing the risk for violence to others (Guy, 2008). However, these accuracy levels resulted mainly from studies on institutional violence and violent recidivism and it should be noted that the accuracy level might drop when predicting events of lower-frequency, which are typical within threat assessment (Meehl & Rosen, 1955).

A few protocols developed specifically for threat assessment purposes exist. Examples are the *Workplace Assessment of Targeted Violence Risk-21* (WAVR-21; White & Meloy, 2010), the *Terrorist Radicalization Assessment Protocol-18* (TRAP-18; Meloy, Roshdi, Glaz-Ocik, & Hoffmann, 2015), and the *Communications Threat Assessment Protocol-25* (CTAP-25; James, MacKenzie, & Farnham, 2014). Although these protocols draw on empirically informed risk factors, they have yet to be extensively evaluated. To my knowledge, no efficacy studies have been published on the CTAP-25 and only one reliability study has been conducted on the WAVR-21 (Meloy et al., 2013). This study revealed excellent interrater agreement for the overall presence of risk factors but a large variability for the presence of individual risk factors. With regard to the TRAP-18, researchers concluded that the protocol appears promising for assessing radicalisation, but that it is not yet sufficiently validated to be utilised as an SPJ instrument (Meloy & Gill, 2016; Meloy, et al., 2015).

In addition to evaluating threat assessment methods, some studies have examined the efficacy of threat management methods. In a study carried out by James and colleagues (2010), 100 consecutive cases from the Fixated Threat Assessment Centre (FTAC) were examined before and after intervention steps were taken. The FTAC is a joint police/health care centre in the UK that was established to assess and manage persons who pose a threat to public figures. The results showed that the level of concern was reduced from moderate/high to low for 80% of the cases (often because health care was offered). Similar success was demonstrated in a follow-up study consisting of a new sample of 100 cases (James & Farnham, 2016). A significant drop in the number of police call-outs, worrisome communication, and approach behaviours was found after (vs. before) FTAC interventions.

On the whole, the efficacy of threat assessment methods is still far from being systematically evaluated. One reason for this is that the field is still relatively young and the amount of data available for such analyses is limited. Another reason is that threat assessment concerns low-frequency incidents, meaning that, for these incidents, there might never be

enough data available in one temporal-cohort to establish predictive accuracy (Gill, Horgan, Corner, & Silver, 2016). Finally, case specific information is often critical when interpreting risk factors. To illustrate, writing a farewell letter can be considered normal behaviour if one is fatally ill but becomes worrisome if the person is in perfect health. As it is impossible to capture all imaginable situations in a threat assessment instrument, it has been argued that threat assessment should be an inductive (or rather abductive) process, meaning that the specific facts of a particular case should guide the inferences made (Meloy et al., 2014a; Reddy et al., 2001). This approach, and related principles, will be discussed in the next section dealing with current practices.

Current Practices

The threat assessment approach that dominates today can be best described as a set of principles widely advocated over time. These principles reflect a mix of logic, professional experience, anecdotes, and research. Some issues discussed below have already been mentioned above but are included again for the sake of providing a complete overview of what is currently considered to be standard practice.

It has been acknowledged that threat assessment is not about predicting who will or will not commit harmful acts but rather about triaging among a number of worrisome cases (Gill, 2015; James & Farnham, 2016). The triage process should result in an assessment of the overall level of concern for potential violence (low, medium, or high). The term “targeted violence” is often used to stress that threat assessment concerns not random violence but rather violence resulting from deliberation (Vossekuil, Fein, & Berglund, 2015). However, some authors make no distinction between targeted violence and other violence as they employ a definition of violence that already includes a certain degree of deliberation (e.g. Douglas et al., 2014). Moreover, violent thoughts and behaviours are primarily shaped by experiences (not personality) and these can change over time and in different situations (Borum et al., 1999). In other words, risk for violence is presumed to be dynamic. This implies that it is critical to identify conditions that bring about a change of risk such as behavioural changes or an upcoming stressful event. It further implies that an assessment holds true only for as long as the conditions under which the assessment was made remain stable (Meloy et al., 2014a, b). Threat assessment professionals must therefore be aware of situational changes and update their work accordingly (Calhoun & Weston, 2015).

For an assessment to be up-to-date, case information must be up-to-date. Information gathering is therefore considered a crucial aspect of threat assessment (van der Meer &

Diekhuis, 2014). The process of information gathering is guided by so-called “key questions” or “need to knows” (Calhoun & Weston, 2015; Vossekul et al., 2015). These questions are supposed to cover all key areas that should be inquired about in order to make a fully informed assessment of a person posing a threat. The questions tap into, among other things, the subject’s motivation, intention, mental health, and capability to cause harm. Explicit threats of violence were found to be an unreliable indicator of risk as many persons who attack utter threats, yet many persons who utter threats do not attack (Warren, Mullen, & McEwan, 2014). Therefore, the common approach dictates that explicit threats should not be ignored and can be a valid reason for making a threat assessment, but they should not necessarily be interpreted as a threshold for concern (Reddy et al., 2001).

Ultimately, threat assessment is meant to identify what types of intervention are needed to mitigate the risks of a particular case. Mitigating threats of violence is referred to as *threat management* and this task is considered equally important as threat assessment (Calhoun & Weston, 2015). Examples of different forms of intervention can be to monitor a subject of concern closely through police surveillance, to arrange security for the potential victim, but also to provide health care and support for the subject. Although threat assessment originated within the context of policing and protecting, a shift has taken place towards a more multidisciplinary approach in which collaboration between police, security, health care, and social services is particularly stressed (e.g. James & Farnham, 2016).

Threat Assessment and Related Fields

This section addresses the field of threat assessment in relation to three intersecting domains of research and practice: violence risk assessment, negotiation, and criminal investigations. It should be noted that the similarities and differences described below are not definite. Instead, while the fields overlap to some extent, the connections between them are subject to change and perspective. This section is not meant as an argument for any particular distinction over another, but rather as an attempt to position the topic of this thesis in a broader context.

Threat assessment vs. violence risk assessment. Risk assessment is a large and established field and it could be argued that threat assessment is one part of it. The fields share an overarching goal: to assess and manage risks for violence. The differences between the two fields stem mainly from the fact that threat assessors and risk assessors *typically* operate in different professional contexts (i.e. law enforcement vs. health care) and they therefore have

different responsibilities. Whether or not the differences exist in practice and whether they are big, small, strict or fluid is debatable (Hart, Hoffmann, de Vogel, & Kropp, 2015). However, as the literature distinguishes between risk assessment and threat assessment, these differences are discussed here (for an overview, see also Meloy et al., 2014a).

Threat assessment takes place in law enforcement/intelligence contexts and the assessments should aid *operational* decision-making (e.g. “Should this stalking victim receive security?”). Importantly, a person of concern in threat assessment is typically moving freely in society. This means that there is a short-term and urgent need to mitigate the risk for violence. Threat assessment professionals are thus required to make rapid assessments based on dynamic and ideographic risk factors (i.e. circumstances that are relevant at this very moment and in this particular case). Risk assessment, on the other hand, often takes place in health care and social services settings and the assessments are meant to aid *legal* decision-making (e.g. “Can this person be safely released from prison?”). The person of concern is typically being detained, meaning that there is no imminent risk for violence. This gives professionals time to collect information and make an assessment, but their assessment is intended to cover a longer time period. As long-term risk for violence is best predicted by static risk factors (e.g. psychopathy, criminal past), historical information is highly informative in risk assessments (Harris et al., 1993).

Threat assessment vs. negotiation. It could be reasoned that if negotiation is needed, it is too late for threat assessment. The task of a threat assessor is to foresee risk acceleration and to intervene before a conflict goes bad. The task of a negotiator is to reach a peaceful resolution when the conflict has already gone bad (Wells, 2015). In other words, threat management is meant to prevent a crisis, whereas negotiation is meant to reduce an ongoing crisis. Threat managers and negotiators are thus *typically* involved at different stages of escalation, which obviously affects their priorities (i.e. information gathering vs. de-escalation, respectively).

That said, professionals in both fields operate in similar domains of violence (e.g. domestic violence, terrorism) and their work concerns similar issues (e.g. mentally unstable subjects of concern coping poorly with life stressors; Rogan, Hammer, & van Zandt, 1994). Engagement with subjects of concern is important in both fields, although more central to the field of negotiation. Literature on both threat assessment and negotiation acknowledges that problem-solving and information gathering during interactions with subjects of concern is best reached through affiliation development (Giebels & Taylor, 2010; van der Meer & Diekhuis,

2014) and that mistakes by the professional may negatively impact the outcome of the interaction (Meloy, 2015; Oostinga, Giebels, & Taylor, 2017). Although, thus far, it is only within the field of negotiation where such acknowledgements have been followed up with scientific research and training on communication methods (e.g. Vecchi, van Hasselt, & Romano, 2005).

Threat assessment vs. criminal investigations. The field of criminal investigation is relevant to threat assessment thanks to its research on suspect interviewing. Threateners and other suspects arguably face a similar dilemma when interacting with law enforcement officials; they need to ensure they are taken seriously without being too specific about their intentions or deeds (Hartwig, Granhag, Strömwall, & Doering, 2010). Understanding the strategies and dilemmas of suspects under interrogation has proven to be of importance for developing successful interview techniques (e.g. Granhag & Hartwig, 2015). The current thesis builds on this line of reasoning.

Research on True and False Intentions

To anticipate risk, it is critical to understand which markers precede future actions. One such marker is intent. Malle and Knobe (1997) defined intent by directly asking people what it means to perform an action intentionally. This resulted in the following: an intended act is an act that one desires, has reasoned about in terms of consequences and skills, has decided upon, and is aware of while performing. The decision can be seen as a commitment or a belief that one is going to act. Intentions are always genuine but people may tell the truth or lie about their intentions. In research on true and false intentions, true intent therefore refers to *statements* about future acts that one truly intends to perform, whereas false intent refers to statements about future acts that one claims, but does not in fact intend to perform (Mac Giolla, Granhag, & Liu-Jönsson, 2013).

However, not all true intentions result in action. Gollwitzer (1999) differentiated between *goal intentions* and *implementation intentions*. Goal intentions reflect what is desired (“I am going to live healthier”), whereas implementation intentions reflect the specifics of when, where, and how the goal should be realised (“I will eat 200 grams of vegetables every evening for the coming six weeks”). Implementation intentions also involve plans for self-regulation, so-called “if-then” plans (“If I am going to dine in a restaurant, then I will have a

salad for lunch”). Gollwitzer (1999) suggested that holding goal intentions does not necessarily lead to goal achievement. Instead, people must operationalise how they intend to achieve their goals and how they will overcome the obstacles they may encounter during goal-striving. This suggestion has received strong empirical support. A meta-analysis revealed that implementation intentions help people to initiate goal-striving, to recognise and exploit goal-congruent opportunities, and keep a course of action by steering away from unwanted influences (Gollwitzer & Sheeran, 2006). Hence, implementation intentions were found to be better than goal intentions at leading to action and goal-achievement. Moreover, persons with no goal intentions were found unlikely to form implementation intentions (Sheeran, Milne, Webb, & Gollwitzer, 2005). These findings imply that implementation intentions may be unique to true intent.

Given that implementation intentions precede behaviour, it would be helpful to threat assessment if implementation intentions could be detected. In broader terms, is it possible to detect true intent? This question is central to a new branch of psycho-legal research grounded in scientific work on deception detection (Granhag, 2010). Instead of examining lies about the past, studies have focused on lies about the future. In a pioneering experiment, passengers in an airport departure hall were asked to either tell the truth or lie during an interview about their upcoming trip (Vrij, Granhag, Mann, & Leal, 2011a). The interviews were coded and judged in terms of veracity. It was found that approximately 70% of statements of intent could be correctly identified as true or false based on the number of plausible details (fewer for liars), contradictions (more for liars), and spontaneous corrections (fewer for liars). A similar level of accuracy was found in a related study that also looked at true and false claims about the future (Vrij, Leal, Mann, & Granhag, 2011b). Although a discrimination accuracy of 70% is nowhere near perfection, it is much higher than results from deception studies on statements about the past (54%; Bond & DePaulo, 2006).

The number of statement details, contradictions, and corrections reflect cues that are studied in traditional lie detection research (Vrij, 2008), but they do not necessarily characterise intent. Subsequent laboratory studies have therefore turned to examining intention-specific cues to deceit. For instance, Ask, Granhag, Juhlin, and Vrij (2013) proposed that true intentions are goal-directed. Drawing on research showing that goal activation leads to positive automatic evaluations of goal-relevant cues (Ferguson & Bargh, 2004), it was predicted (and found) that persons who truly intend to achieve a particular goal evaluate cues relevant to this goal more positively as compared to persons with false intent (Ask et al., 2013). Moreover, planning is considered a defining feature of true intent (Granhag, 2010) and planning is related to the ability

to imagine future scenarios (Szpunar, 2010). Researchers who addressed the link between true intent and pre-experiencing the future found that persons were indeed more likely to activate mental images when they planned for an activity they truly (vs. falsely) intended to carry out (Granhag & Knieps, 2011; Knieps, Granhag, & Vrij, 2013).

These findings are theoretically relevant as they suggest that different cognitive processes underpin true and false intent. However, cognitive cues such as positive evaluations and mental images are not often observable to outsiders and therefore cannot directly aid threat assessment. Of more practical relevance is whether or not markers of true intent exist that are detectable for professionals charged with assessing intent (e.g. border security personnel). For instance, does the truth reveal itself in statements about intent?

Drawing from the *Construal Level Theory* (CLT; Trope & Liberman, 2010), it could be argued that people should talk about true intentions more concretely (as opposed to abstractly). CLT was originally developed to explain how people mentally represent past and future situations such as memories, speculations, hopes, and intentions. These mental representations are called construals and range from more concrete to more abstract. Concrete construals typically reflect the feasibility of an action (i.e. *how* to act), whereas abstract construals typically reflect the desirability of an action (i.e. *why* to act; Trope & Liberman, 2010; Vallacher & Wegner, 1987). CLT holds that construals become more concrete when they concern events that are more psychologically proximate to oneself. Psychologically proximate events are those that will take place in the near future (temporal proximity), at a location close by (spatial proximity), apply to oneself (social proximity), or are certain to happen (hypothetical proximity). Importantly, CLT proposes that the level of abstraction in mental representations affects people's behaviours, evaluations, and predictions of events. Such secondary effects of mental abstraction levels are called "downstream consequences." Numerous experiments have examined the assumptions of CLT and support has been found for the effect of psychological proximity on the abstraction levels of both mental representations and downstream consequences (Soderberg, Callahan, Kochersberger, Amit, & Ledgerwood, 2014). These effects were found to be robust across time, research labs, and populations.

When studying intentions (or threats), hypothetical proximity is particularly relevant. After all, a person who holds a true intention has decided to act, in contrast to a person who holds a false intention. Research has shown that proximity differences can reveal themselves in verbal statements. That is, people describe activities in more concrete terms when the activity is to happen soon (Liberman & Trope, 1998) and when the activity is more likely to occur (Wakslak, Trope, Liberman, & Alony, 2006). Thus, it could be theorised that statements of true

intent (e.g. true threats) are coloured by concrete how-related details, whereas statements of false intent (e.g. bluffs) by comparison are characterised more by abstract why-related details.

A series of studies have provided tentative support for this theory using variants of the following experimental paradigm (Granhag & Knieps, 2011). Participants were assigned the role of truth teller or liar. Truth tellers were given a neutral task to plan and carry out (e.g. gift shopping) while liars were given a mock crime to plan and carry out (e.g. hiding a USB-stick containing illegal material in the shopping centre). In addition, liars were told to prepare a cover story in case they were apprehended. The cover story resembled that of the truth tellers' task and thus reflected a statement of false intent. After planning, but before executing their tasks, participants were apprehended and interviewed about their intentions. Truth tellers gave a truthful account, whereas liars told their cover story. Their statements were then analysed for markers of true and false intent.

Results of these studies have shown that truth tellers provide comparably more information on *how* to implement their goal, whereas liars provide comparably more information on *why* to implement their goal (Mac Giolla, et al., 2013; Sooniste, Granhag, Strömwall, & Vrij, 2014; Sooniste, Granhag, Strömwall, & Vrij, 2015). Moreover, studies have revealed that truth tellers provide longer and more detailed answers to unanticipated questions about planning (Mac Giolla & Granhag, 2015; Sooniste, Granhag, Knieps, & Vrij, 2013; Sooniste et al., 2014; 2015), are more likely to mention time management issues (e.g. "Let us split the group and divide the tasks"), and more often foresee potential problems pertaining to their future task (Mac Giolla et al., 2013). For a review of psycho-legal studies on true and false intentions, see also Granhag and Mac Giolla (2014).

Research on Human Intelligence Interviewing

Human Intelligence

Human intelligence (HUMINT) can be described as information collected by professionals through interactions with one or more persons (Justice, Bhatt, Brandon, & Kleinman, 2010). HUMINT gathering is considered a core component of law enforcement work and counter-terrorism efforts (Vrij & Granhag, 2014). HUMINT can be used as evidence in a court of law if it is acquired in accordance with country-specific rules of evidence (e.g. the Fifth Amendment in the US). However, the literature typically distinguishes between evidence and HUMINT (Evans, Meissner, Brandon, Russano, & Kleinman, 2010). Evidence is information

that contributes to the conviction (or acquittal) of a suspect, whereas HUMINT is defined as information that can be used to improve local or national security. Moreover, HUMINT (as opposed to evidence) is typically gathered outside custodial settings on a voluntary basis, can take place over the course of months or years, and can contain a covert component (for an overview of similarities and differences between HUMINT and evidence, see Evans et al., 2010). The information obtained with TAM interviewing can be seen as HUMINT as it is typically used to evaluate the likelihood of an individual to commit acts of violence and, then, to prevent this from happening. Most research on investigative interviewing has focused on collecting evidence rather than HUMINT (Evans et al., 2014). The 9/11 attacks resulted in a shift of interest, but the impact of behavioural science on policies and practices within intelligence agencies long remained limited (Brandon, 2011). Emerging research on intelligence gathering is now gradually filling this knowledge gap (for a recent review of research, see Meissner, Surmon-Böhr, Oleszkiewicz, & Alison, 2017). Two research topics concerning HUMINT gathering may be particularly relevant to TAM interviewing: counter-interview strategies and interview methods.

Counter-Interview Strategies

Counter-interview strategies can be described as all efforts by interviewees to manage the information they hold and to regulate the way they present themselves in interviews (Hartwig et al., 2010). The focus in this thesis is on *verbal* counter-interview strategies, which concerns the interviewee's spoken communication with the interviewer. Such strategies can be generated by the interviewees themselves or result from instructions given to them by others. In both cases, counter-interview strategies are ways to steer one's own behaviour towards desired interview outcomes, which can be seen as a form of self-regulation (Fiske & Macrae, 2012). The need for self-regulation increases in aversive situations with uncertain outcomes (Fiske & Macrae, 2012). Legal interviews (whether these involve suspects, sources, or threateners) are typically uncertain and aversive situations because there are risks involved for the interviewee, such as the risk for prosecution (suspect), the risk for retaliation (source), or the risk for interference with plans (threatener). Hence, counter-interview strategies should be expected in such settings.

A study of real-world interrogations revealed that terrorist suspects did indeed make use of counter-interview strategies and that the type of strategies used, differed across different terrorist groups (Alison et al., 2014a). For instance, Al-Qaeda inspired terrorists used retraction tactics (i.e. retracting previous statements) significantly more than right wing terrorists and

paramilitary groups, the latter of which more often responded to interrogations with passive responses (e.g. remaining silent, no-comment response) or by providing irrelevant information, embedded lies, or scripted responses. The use of such strategies reflects manuals produced by these terrorist groups (e.g. the Al-Qaeda training manual; the IRA Green Book). In these manuals, members are advised to anticipate the interview techniques employed by the police or to say nothing during interrogations.

In addition to operational findings, experimental research has been conducted on counter-interview strategies with mock suspects. According to theory and research on self-presentation, guilty and innocent suspects are equally motivated to make a credible impression (DePaulo, 1992; Hartwig et al., 2010). However, to avoid prosecution, guilty suspects must conceal the truth, whereas innocent suspects must reveal the truth. This difference is presumed to result in avoidant versus forthcoming counter-interview strategies, respectively. In support of this presumption, research has shown that guilty suspects are more concerned with maintaining control and thereby adopt avoidant strategies (e.g. avoiding incriminating details, keeping it simple), while innocent suspects are more concerned with providing correct information thereby adopting forthcoming strategies (e.g. telling the truth like it happened; Hines et al., 2010; Strömwall, Hartwig, & Granhag, 2006). Moreover, guilty suspects compared to innocent suspects (i) tend to use more (and more diverse) strategies (Hartwig, Granhag, & Strömwall, 2007), (ii) are more aware of the risk for not being believed (Hartwig et al., 2010) and (iii) react more strongly to the possibility that there might be evidence against them resulting in pronounced withholding or pronounced forthcoming counter-interrogation strategies (Luke, Dawson, Hartwig, & Granhag, 2014).

To develop effective interview techniques (including tactical approaches to detect deceit), it is essential to learn about interviewees' counter-interview strategies. Such knowledge improves the interviewer's ability to take perspective and consider the world from someone else's viewpoint (Galinsky, Maddux, Gilin, & White, 2008). Perspective taking allows for anticipation of the behaviour of others and professionals in legal settings could incorporate this skill into their interview techniques. They could use techniques that exploit the counter-interview strategies of both truth tellers and liars to elicit cues that are indicative of guilt or innocence. Moreover, they could use techniques that reduce the use of counter-interview strategies by semi- or non-cooperative interviewees to elicit more information (Granhag, Hartwig, Mac Giolla, & Clemens, 2015). Such techniques are referred to as strategic interviewing techniques; see the next section for an elaboration on this type of interviewing.

Interview Methods

Methods for investigative interviewing and interrogation can be divided into three broad categories: confession-oriented (or accusatorial) methods, information-gathering methods, and strategic interviewing methods (Hartwig, Luke, & Skerker, 2016). *Confession-oriented methods* are aimed at producing confessions. Police interrogation manuals (e.g. Inbau, Reid, Buckley, & Jayne, 2011), observational studies (e.g. Leo, 1996), and controversial war practices have revealed that this is often achieved using techniques that involve physical or psychological manipulation. Confession-driven interviewing is highly criticised within the research community. Not only does the method rest on an incorrect assumption of guilt (i.e. the suspect may be innocent), but the tactics are also considered immoral as they violate the suspect's autonomy and consent (Hartwig et al., 2016). Finally, there is no scientific support for the efficacy of confession-driven interviewing, the method was even found to increase the likelihood of false confessions (Meissner et al., 2014). While such interview methods are still practiced around the world, several countries have adopted laws and interview standards that instead promote an information-gathering approach (e.g. Home Office 2003; Milne, Shaw, & Bull, 2007).

Information-gathering methods aim at eliciting a complete and reliable account from the subject. This is done by establishing rapport and by using open-ended questions as well as direct, positive confrontations (Meissner et al., 2014). When information-gathering methods are used for deception detection, the focus is on eliciting cues to deceit that result from cognitive (rather than emotional) differences between truth-tellers and liars (Vrij & Granhag, 2014). One advantage of information-gathering methods over confession-driven methods is that the former build on theories of how people memorise and communicate information (Milne et al., 2007). A meta-analysis of experimental studies demonstrated the positive effects of information-gathering interviewing: the likelihood of true confessions was preserved and, in some cases, increased (Meissner et al., 2014). Additionally, information-gathering methods reflect ethical progress, as the methods emphasise honesty, transparency, and respectful treatment of the suspect (Hartwig et al., 2016).

When testing the comparative efficacy of information-gathering methods on information elicitation, a distinction can be made between *direct interviewing* and *rapport-based interviewing*. Direct interviewing is the most basic information-gathering approach in which open-ended questions are asked in a business-like manner (Justice, et al., 2010). Rapport-based interviewing is comparatively more advanced and can be described as a friendly interview style characterised by acceptance, empathy, and respect for the interviewee's

autonomy (Alison, et al., 2014b; Saywitz, Larson, Hobbs, & Wells, 2015). Bull (2013) reviewed literature on characteristics that contribute to skilled investigative interviewing and concluded that the best information gatherers are those who can establish and maintain rapport throughout the interview. For instance, it was found that rapport-based interviewing reduced suspects' use of counter-interview strategies (Alison, et al., 2014a), and led to an increased information yield (Alison, Alison, Noone, Elntib, & Christiansen, 2013). These findings match field research in which offenders were found more willing to provide truthful accounts in response to humane, honest, non-dominant, and respectful interviewing (Kebbel, Hurren, & Mazerolle, 2006; O'Connor & Carson, 2005).

The most recent developments in human intelligence interviewing concern *strategic interview methods*. These methods go beyond information-gathering as they rest on the belief that a skilled interviewer understands and exploits the counter-interview strategies of the interviewee (Granhag et al., 2015). One example of strategic interviewing is to play on the expectations of the interviewee by asking unanticipated questions. Liars have been found to perceive it to be more difficult to answer such questions because they cannot draw from true experiences while truth-tellers can (Vrij et al., 2009). Another technique is the Strategic Use of Evidence (SUE) technique that builds on the notion that both guilty and innocent suspects must reveal information to be perceived as credible, but that only guilty suspects must also conceal information to avoid self-incrimination (Granhag & Hartwig, 2015). The interviewer may exploit the conflicting mind-set of guilty suspects by withholding evidence from them, which leads guilty suspects (more than innocent suspects) to make statements that contradict the evidence (Hartwig, Granhag, & Luke, 2014). Moreover, strategic interview tactics have been developed to elicit information from interviewees while masking the aim of the interview, the so-called Scharff-technique (Oleszkiewicz, 2016). An interviewer using the Scharff-technique creates the illusion that s/he already knows all information interviewees hold, leading interviewees to believe they can reveal their information safely. Furthermore, the interviewer presents claims that only need to be confirmed or disconfirmed. This tactic enables the interviewer to elicit valuable information via a short (dis)confirming response only. Finally, by not pressing for information and showing little interest in new and critical information, the interviewer can hide from interviewees what information s/he is after. These tactics are considered particularly relevant for eliciting information in intelligence operations. Recent empirical work has provided support for the efficacy of the Scharff-technique (Granhag, Kleinman, & Oleszkiewicz, 2016).

A Novel Experimental Paradigm

This thesis introduces a novel experimental approach with respect to TAM interviewing. Since planned acts of violence are extreme behaviours that occur infrequently, experimental research is uncommon in the field of threat assessment and management. Some may argue that high-stakes events cannot be investigated in a laboratory as artificial setups would limit the generalisability of the results. In this section, an explanation is given of why the employed experimental approach was chosen and how research based on this approach can contribute to existing knowledge on threats of violence.

One lesson learned from anecdotal studies is that every threat case is different. However, managing such cases can be done systematically. The studies in this thesis do not investigate individual characteristics of threat cases, but rather the process of human intelligence gathering to assess and manage threats. As noted in the previous section, human intelligence gathering is nothing more than collecting information through interactions with people (Justice et al., 2010). Human intelligence gathering can therefore be viewed in the context of social and cognitive psychology (Evans et al., 2010). It is safe to assume that fundamental social and cognitive processes function similarly across populations. For instance, the avoidance-approach motivation (i.e. the motivation to approach positive stimuli and avoid negative stimuli) is central to human functioning and relates to important dilemmas and decisions that threateners face, such as to accept or reject a loss, to reveal or conceal information, and to follow through on a threat or not (Eliot, 2008). Moreover, applied research has shown that extremists commonly leave violence behind for very ordinary reasons such as burnout, feelings of guilt, missing loved ones, or longing for a normal life (Dalgaard-Nielsen, 2013). Even when dealing with persons with mental illnesses, it was found that simple matters such as helping them obtain social security benefits were effective in reducing risk (James & Farnham, 2016). These findings illustrate that despite deviant behaviours, the needs and drives of those who pose a threat might not differ from those who do not. This presumption, among other things, merits laboratory studies on threat management using a normal population.

Furthermore, experimental research may contribute to a deeper understanding of the techniques underpinning threat management skills. Understanding a skill is not necessary to possess that skill; people can be good at something without knowing what exactly makes them good at it. The understanding, though, becomes important when teaching others. For instance, Hans Scharff was considered an outstanding WWII interrogator of the German Luftwaffe

(Toliver, 1997), but it was only 75 years later that his skills were taught to law enforcement professionals (Oleszkiewicz, Granhag, & Kleinman, 2017). This development is due to the fact that researchers became inspired by anecdotal evidence of Scharff's effectiveness, then identified his tactics and tested them in laboratory studies (Oleszkiewicz, 2016). On a more general note, extensive research on interview techniques has led some police and intelligence services to take part in training sessions on science-based methods of interrogation (Meissner et al., 2017) and to adopt science-based frameworks for interviewing suspects (e.g. the PEACE model; Milne et al., 2007), for interviewing eyewitnesses and victims (e.g. Cognitive Interview; Memon, Meissner, & Fraser, 2010), and for communicating in crisis situations (e.g. the Behavioral Change Stairway Model; Vecchi et al., 2005). Researchers within these fields have to deal with similar challenges regarding external validity as researchers within the field of threat assessment. However, such challenges have not deterred them from conducting experimental research or, more importantly, from translating research to practice and policy.

That said, it is important to strike a balance between experimental control and external validity by mirroring critical real-life aspects in the lab. As a result, the following matters were addressed in the paradigm employed in this thesis. First, the act of threatening can be considered deviant behaviour, but it is reasonable to think that a person who makes a threat finds it acceptable (e.g. "I have no other choice" or "I must fight injustice"; Dalgard-Nielsen, 2013). To reflect this mind-set, the case given to participants was phrased in such a way that they represented the party who was morally right according to widely accepted values, threatening a party who was morally wrong. Second, the act the participants threatened to commit was not physically violent (for obvious ethical reasons), but was still damaging. For instance, participants threatened to leak information to the media or press charges in order to cause financial or reputational damage to a company. Third, in order to establish true intent, participants were led to believe they really could carry out the threat. Of course, participants understood this act was part of the role-play, but the critical part was that they truly believed they were going to follow their threat up with an act (e.g. delivering a USB-stick to an accomplice containing damaging video recordings). Fourth, emotional involvement was established via the content of the case (i.e. fighting injustice) and via the nature of the task (i.e. performing the fairly nerve-wracking act of interacting with an unknown person about conflicting interests). Fifth, the dependent measures of the studies were selected based on their practical value to threat assessment and management. Measures included for threat assessment purposes were the type, amount, and timing of the information provided by threateners during the interviews as well as their use of counter-interview strategies. As pertains to threat

management, the threateners' willingness to carry out a threat was measured as well as their willingness to communicate with professionals about the threat.

CHAPTER 2: SUMMARY OF EMPIRICAL STUDIES

This thesis includes four empirical studies. Three of these are laboratory experiments (Studies I, II, III) and the fourth is an online passive-observational study (Study IV). The methodological parameters of the studies are summarised in Table 1. In the laboratory experiments, participants were interviewed about a threat they had made. The information provided during the interview (e.g. amount, type), the counter-interviewing strategies reported to have been used (e.g. type, change in strategy), and attitudes towards the threat and the interview (e.g. willingness to carry out the threat) were examined. The aim of these studies was to investigate how interviewing can contribute to threat assessment and management goals such as differentiating between bluffers/actualisers and increasing information yield. In the online study, threat assessment professionals and non-professionals assessed the risk for violence in fictitious cases. This study sought to examine how professional experience contributes to the quality of threat assessments.

Table 1

Overview of Studies Constituting this Thesis

Study	Method	N	k	Independent Variables	Dependent Variables
I	Lab Experiment	157	3	Threat Intent (bluffer vs. conditional actualiser vs. decisive actualiser)	Information Provision Time of Disclosure
II	Lab Experiment	179	4	2 Threat Intent (bluffer vs. actualiser) × 2 Interview Protocol (high vs. low suspicion)	Information Provision Time of Disclosure Strategy Use
III	Lab Experiment	120	2	Interview Protocol (direct vs. rapport-based)	Information Provision Strategy Use Willingness to Carry out Willingness to Interact
IV	Online Passive- observational	133	3	Professional Experience (professionals vs. students vs. laymen)	Agreement Information Search

Note. N = participants, k = conditions.

Study I

Study I introduced an experimental paradigm for studying verbal threats. The study examined whether true or false intent to actualise a threat manifests in the verbal content of the threat. Simply put, do persons with true intent to actualise threats (actualisers) formulate threats differently than persons without intent to actualise threats (bluffers)? Drawing on literature on true and false intent, it was predicted that threats reflecting true intent would be accompanied by comparatively more implementation details (*how* the threat will be actualised), whereas bluffs would be concentrated more on the formation of ideas (*why* the threat is posed). This prediction was based on the finding that people think and talk more concretely about events that are more likely to happen (Wakslak et al., 2006). Intent was manipulated across three conditions via the likelihood to actualise the threat: low likelihood (no intent: *bluffers*), medium likelihood (weak intent: *conditional actualisers*), and high likelihood (strong intent: *decisive actualisers*). It was predicted that decisive actualisers would provide the most how-related information, followed by conditional actualisers, and bluffers, who would provide the least. No differences were expected with respect to the amount of why-related information disclosed. Furthermore, the point of the interview at which participants provided the most information was also explored. Did participants reveal more information in response to information-seeking questions (earlier in the interview) or in response to challenging questions (later in the interview)? The manuscript of Study I was published in the *Journal of Threat Assessment and Management* (see Appendix E).

Method

Participants and design

One hundred and eighty one students (128 women, 53 men; $M_{age} = 28.31$ years, $SD = 10.05$ years) at the University of Gothenburg (Sweden) participated in the study. Participants were recruited via the university participant pool. This pool consists of both students and non-students who have signed up for participation in psychological research. Participants were approached via email and asked to take part in a study on campaigning strategies used by Non-Governmental Organisations (NGO). They received a cinema ticket for participation (worth approximately €1). Participants were randomly assigned to one of three experimental conditions: bluffers, conditional actualisers and decisive actualisers. Seven persons felt uncomfortable making a threat and withdrew from the study. Seventeen participants did not correctly follow the instruction to act or not to act on their threat. Eleven of these had

misunderstood or forgotten this part of the instruction, and six did not believe that they were truly supposed to follow through with the threat. Their data were excluded from further analysis. A total of 157 participants thus remained: 54 bluffers, 51 conditional actualisers and, 52 decisive actualisers (108 women, 49 men; $M_{age} = 28.10$ years, $SD = 9.67$ years).

Procedure

Participants were tested individually. The same case was presented to all participants. It reflected a moral conflict between a fictive Non-Governmental Organisation (NGO) named Aweare and a fictive clothing company named Vera. Participants read how Aweare was dedicated to improving working conditions in low-wage countries and how Vera was known as being socially engaged in the local communities in the countries to which they outsource their production. Vera had recently released a commercial in which they drew attention to violence against women. Meanwhile, Aweare got hold of video recordings showing how Vera exploited women in factories in Cambodia. Aweare considered it to be hypocritical for Vera to raise public awareness about violence against women while simultaneously exploiting them for their own profit. Aweare therefore decided to take action against Vera. Participants were instructed to imagine being part of Aweare and to represent Aweare in this action.

All participants were instructed to call a representative of Vera and to threaten that they would leak the video recordings with evidence of Vera's malpractice to a Swedish television programme for investigative journalism, if the company would not withdraw their commercial from television. Participants were either instructed not to leak the recordings (bluffers), to leak the recordings only if the company would not agree to withdraw their commercial (conditional actualisers) or to leak the recordings no matter how the company would respond to their threat (decisive actualisers). All participants were left alone for 15 minutes to prepare for their task(s) and all had access to the same background materials. These materials included both 'why' related information (e.g. visions of Aweare, working conditions in Cambodia) and 'how' related information (e.g. delivery location for the recordings, name of the media contact). Participants were allowed to make notes and to have those with them while talking to Vera.

Next, the participants called the representative of Vera. They were led to believe that the person on the other end of the phone was another participant instructed to play the role as the representative. In reality, however, the recipient of the call was a confederate, who responded to the threats exactly the same for each participant, using four different questions/prompts:

Q1: *Hello, this is Caroline. I'm the head of Public Relations at Vera and I expected your call. You initiated this conversation, so please go ahead.*

Q2: *I'm not sure I fully understand what you mean; can you please give me more information?*

Q3: *How do I know that what you are telling me is true?*

Q4: *Is there anything else I should know about before ending the conversation?*

Okay, let me think about this. Thank you for your input. Bye.

After the conversation, the experimenter informed the participants that the Vera representative thought they were bluffing and therefore decided to ignore the threat. They were then instructed to proceed with their task according to the instructions. Bluffers were supposed to do nothing, whereas both conditional and decisive actualisers were supposed to provide their media contact with a USB stick containing the video recordings. They were intercepted immediately after starting the implementation (e.g. put on their coat, walked towards the door).

Before the participants made the call, they rated nine statements on their involvement with the case (e.g. "I consider women rights and poverty reduction to be two of the most important priorities for NGO's to focus on", 1 = *strongly disagree*, 7 = *strongly agree*) and their motivation to perform their task (e.g. "I want Vera to believe that my threat is real"; 1 = *strongly disagree*, 7 = *strongly agree*) using Likert scales. After the call and the interception, the participants rated the clarity of the instructions ("How easy/difficult did you find the instructions?"; 1 = *very difficult*, 7 = *very easy*), their satisfaction with the preparation time (1 = *not at all sufficient*, 7 = *very sufficient*), the amount of preparation time spent on preparing for the call (1 = *no time at all*, 5 = *all the time*), the amount of preparation time spent on preparing for the delivery (1 = *no time at all*, 5 = *all the time*) and the credibility of the set up (e.g. "To what extent did you believe that you would deliver the USB stick to a contact person"; 1 = *very unlikely*, 7 = *very likely*). Participants were then thoroughly debriefed, thanked and paid for their participation.

Codings and data preparation

All calls were transcribed verbatim and coding was conducted on these transcriptions. Two coders, blind to the conditions and the hypotheses, first identified 'how' and 'why' information in the background materials that participants had access to while preparing for the call. The coders relied on Liberman and Trope's (1998) distinction between desirability (why) and feasibility (how). All information that related to the operations of Vera, the operations of

Aware, the released commercial, and human rights in general was identified as ‘why’ information. All information that related to the video recordings, the delivery procedure, the delivery location, and the possibilities to successfully implement the threat via investigative journalism or Aware, was identified as ‘how’ information. In total, 44 pieces of ‘why’ information and 32 pieces of ‘how’ information were identified in the background materials. Each transcript was then coded for the amount of unique pieces of ‘how’ information (range: 32) and ‘why’ information (range: 44). Each piece of information was counted only the first time it was mentioned by the participant and repetitions were thus not taken into account. To assess the interrater reliability, one coder coded all the transcripts and the other coder coded 20% of the transcripts. The interrater agreement was 90 % (Cohen’s $\kappa = .71$).

To explore at which point in time during the interview participants disclosed their information, a new dependent measure was computed for ‘how’ and ‘why’ information, respectively, using the following equation:

$$T_{av} = \frac{n_1(1) + n_2(2) + n_3(3) + n_4(4)}{N}$$

Where T_{av} = the average time (within the interval ranging from Question 1 to 4) when the information was reported, n_i = the number of pieces of information revealed at the i th question, and N = the total number of pieces of information revealed across all four questions. The measure could thus range from 1 (all information revealed at Q1) to 4 (all information revealed at Q4).

Results

Self-ratings

Self-ratings on 7-point Likert scales showed that the participants believed in the setup ($M = 4.96$, $SD = 1.07$), were involved with the case ($M = 5.59$, $SD = 0.77$), and were highly motivated to make a convincing threat ($M = 6.25$, $SD = 0.92$). Moreover, they did not find it overly difficult to comply with the instructions ($M = 4.99$, $SD = 1.47$), experienced sufficient time to prepare for their tasks ($M = 4.53$, $SD = 1.72$), which they had largely spent preparing for the threat call ($M = 4.26$, $SD = 0.79$, rated on a 5-point scale). Analysis of variance (ANOVA) revealed no significant differences between conditions on the above measures. The only pre-threat measure that showed differences between the conditions was the reported time spent on preparing for the delivery of the USB stick, $F(2, 146) = 16.52$, $p < .001$, $\eta^2 = .18$. A

post hoc test, using Bonferroni-corrected alpha levels, revealed that bluffers reported significantly less preparation time spent on the delivery ($M = 1.20$, $SD = 0.06$) than both the conditional actualisers ($M = 1.98$, $SD = 0.14$, $p < .001$) and the decisive actualisers ($M = 2.02$, $SD = 0.13$, $p < .001$). This finding can be seen as an additional manipulation check, as bluffers were not supposed to deliver the USB stick. When participants were asked in the debriefing to express their thoughts about the study, many spontaneously mentioned that they were nervous to make the call (48%), that the task was demanding (34%), and that the set-up felt real (26%).

Hypothesis testing

The distributions of both ‘how’ and ‘why’ scores were negatively skewed ($skewness_{\text{how}} = 0.70$, $SE = 0.19$; $skewness_{\text{why}} = 1.63$, $SE = 0.19$) and leptokurtic ($kurtosis_{\text{how}} = 0.64$, $SE = 0.39$; $kurtosis_{\text{why}} = 5.53$, $SE = 0.39$). Hence, we conducted non-parametric analyses to test our hypothesis. The descriptive statistics for each of the experimental groups are reported in Table 2 (top panel).

To test for the predicted trend across conditions, individual scores were ranked and analyzed using the Jonckheere test (Jonckheere, 1954). A significant trend in the ‘how’ data was found. However, the conditions were ranked in the opposite direction to that predicted. The highest group median was found for bluffers, followed by conditional actualisers and decisive actualisers, $J = 3300$, $z = -2.61$, $p = .009$, $r = -.21$. In other words, the group that was least likely to actualise the threat (bluffers), was found to provide the most ‘how’ information. Follow-up analysis, using Mann-Whitney tests with a Bonferroni correction, showed that bluffers provided significantly more ‘how’ information during the threat call than did decisive actualisers, $U = 971$, $z = -2.75$, $p = .006$, $r = -.27$. No significant difference was found between bluffers and conditional actualisers ($U = 1162$, $z = -1.38$, $p = .167$, $r = -.13$) or between decisive and conditional actualisers ($U = 1166.5$, $z = -1.06$, $p = .290$, $r = -.10$). With regard to the amount of ‘why’ information provided during the threat calls, no significant difference between conditions was found using the Kruskal-Wallis test, $X^2(2, N = 157) = 0.56$, $p = .76$, $\eta^2 = .00$.

Exploratory analyses

To examine the point in time during the interview at which participants disclosed their information, we conducted a Kruskal-Wallis analysis on the average timing of information disclosure. Descriptive statistics are reported in Table 2 (bottom panel). The analysis revealed that the timing of disclosure of ‘how’ information differed between the conditions, $X^2(2, N =$

157) = 8.85, $p = .012$, $\eta^2 = .06$. Pairwise Mann-Whitney comparisons, using Bonferroni-corrected alpha levels, revealed that bluffers disclosed ‘how’ information significantly later in the interview than did decisive actualisers, $U = 944.5$, $z = -2.91$, $p = .004$, $r = -.28$. No significant differences were found between bluffers and conditional actualisers ($U = 1127$, $z = -1.60$, $p = .109$, $r = -.15$) and between conditional and decisive actualisers ($U = 1104$, $z = -1.47$, $p = .143$, $r = -.15$). A similar pattern was observed for the timing of ‘why’ information. The point in time during the interview at which participants disclosed ‘why’ information differed between conditions, $X^2(2, N = 157) = 11.58$, $p = .003$, $\eta^2 = .07$. Bluffers disclosed ‘why’ information significant later in the interview than did conditional actualisers ($U = 917$, $z = -2.95$, $p = .003$, $r = -.29$) and decisive actualisers ($U = 943.5$, $z = -2.91$, $p = .004$, $r = -.28$). No significant difference was found between conditional and decisive actualisers ($U = 1346$, $z = .13$, $p = .895$, $r = .01$).

Table 2

Descriptive Statistics for the Amount (Top Panel) and Timing (Bottom Panel) of ‘Why’ and ‘How’ Information Revealed by Bluffers, Conditional Actualisers, and Decisive Actualisers.

Condition	Why			How		
	<i>M (SD)</i>	95% CI	<i>Mdn</i>	<i>M (SD)</i>	95% CI	<i>Mdn</i>
Amount						
Bluffers	8.31 (3.29)	[7.42, 9.21]	8.00	8.80 (3.18)	[7.93, 9.66]	9.00
Conditional	8.18 (3.74)	[7.13, 9.23]	8.00	8.35 (4.07)	[7.21, 9.50]	7.00
Decisive	8.35 (4.86)	[6.99, 9.70]	7.00	7.25 (3.17)	[6.37, 8.13]	7.00
Time						
Bluffers	1.81 (0.40)	[1.70, 1.92]	1.80	2.40 (0.78)	[2.19, 2.62]	2.33
Conditional	1.58 (0.45)	[1.46, 1.71]	1.50	2.17 (0.74)	[1.97, 2.38]	2.10
Decisive	1.58 (0.42)	[1.46, 1.70]	1.50	1.98 (0.76)	[1.77, 2.19]	1.85

Note. The time variables correspond to the average point in time during the interview at which the information was revealed (1 = all information revealed at Question 1, 4 = all information revealed at Question 4).

All interviews started with two information-seeking questions/prompts (Q1: “Please go ahead” and Q2: “Can you please give me more information”), followed by two challenging question (Q3: “How do I know that what you are telling me is true?” and Q4: “Is there anything else I should know about before ending the conversation?”). The patterns of change in responses from the information-seeking phase (Q1 and Q2) to the challenging phase (Q3 and Q4) differed significantly between the experimental conditions. More specifically, 44% of the bluffers revealed more ‘how’ information in the challenging phase than in the information-seeking phase, compared with 23% of the conditional actualisers, and 17% of the decisive actualisers, $X^2(2, N = 157) = 9.67, p = .008, \eta^2 = .06$. Again, pairwise comparisons only revealed significant differences between bluffers and decisive actualisers ($p = .007, r = .30$). No difference was found with respect to ‘why’ information. Participants in all conditions showed similar patterns of change in their ‘why’ response. Only 2% of the bluffers, 2% of the conditional actualisers, and 2% of the decisive actualisers revealed more ‘why’ information in the challenging phase than in the information-seeking phase, $X^2(2, N = 157) = 0.35, p = .839, \eta^2 = .00$.

Gender

Female participants ($M = 5.70, SD = 0.61$) reported a significantly higher involvement with the case, compared to male participants ($M = 5.33, SD = 0.99$), $t(155) = 2.916, p = .004, d = .44, 95\% CI [.09, .78]$. However, no significant Gender \times Condition interactions were found for the amount and timing of how-information provided and for the amount and timing of why information provided (all p 's $> .279$). This means that the manipulation of the study (i.e., random assignment of participants as bluffers, conditional actualisers, or decisive actualisers) affected male and female participants similarly.

Discussion

Contrary to the hypothesis, participants who were least likely to actualise the threat (bluffers) provided the most detail on how the threat would be implemented. This finding became particularly pronounced when participants were challenged in the latter half of the interview, that is, when they were questioned critically (“How do I know what you are telling me is true?”) or given a last opportunity to talk (“Is there anything else I should know about before ending this conversation?”). The groups did not differ in terms of the disclosure of why-related information. Overall, bluffers revealed more information during the latter half of the interview as compared with decisive actualisers.

These results contradict previous studies which suggest detailed accounts of planning and implementation are associated with true intent (Mac Giolla et al., 2013; Sooniste et al., 2014) and the risk that threats will be actualised (Calhoun & Weston, 2003). Furthermore, the results conflict with the notion that events likely to happen in the near future are construed and described in more concrete, how-related terms (Wakslak et al., 2006). A potential explanation may be that actualisers, more often than bluffers, choose to keep how-related details to themselves to ensure successful implementation. This explanation suggests that threat statements reflect strategic concerns about what is *best* to reveal rather than what is *possible* to reveal. Differently put, threateners must strike a balance between what information to reveal and what information to conceal. Threat managers may benefit from learning more about such information-management strategies.

A few limitations should be mentioned. First, the verbal behaviours of bluffers and decisive actualisers did not differ significantly from that of conditional actualisers. This might have been due to the manipulation. The likelihood to actualize the threat (deliver USB stick) was manipulated between conditions. However, the likelihood to make the threat was the same for all three conditions (all participants had to make the phone call). Because participants were generally nervous for making the call and spent most of the preparation time preparing for this, less thoughts and effort might have gone to the actual manipulation (i.e., delivering the USB stick or not). If this was the case, the conditions did not differ too much from each other and the study failed to manipulate the participants' construals and subsequent behaviours. Second, the generalizability of the current findings might be limited by the overrepresentation of females in the tested sample and by limited personal involvement of the participants in the threats they made. Although participants in the current study reported that they felt involved in the case, that they were motivated to perform well, and that they experienced participation as real and demanding, an experimental setting obviously differs from the more complex circumstances in which threatening behaviour commonly occurs (e.g., grievance, hostile world views, mental illness; Warren et al., 2013).

Study II

The second study elaborated on the idea that emerged in Study I. That is, in order to elicit valuable information from threateners, it is important to learn about the strategies they employ when being questioned about their intentions (i.e. counter-interview strategies).

Understanding the counter-interview strategies of interviewees has proven to be of great value in related settings such as suspect interviewing and human intelligence gathering (Granhag & Hartwig, 2015; Oleszkiewicz, Granhag, & Cancino Montecinos, 2014). In Study II, it was explored whether threatening participants used counter-interview strategies or not, whether they changed strategies during the interview or not, and why they changed strategies (for those who did). Additionally, it was theorised that the need to be believed is more urgent for bluffers than for actualisers as bluffers are entirely dependent on a target's willingness to meet their demands. Based on this assumption, it was predicted that bluffers (in comparison to actualisers) would be more forthcoming when asked specific questions (Hypothesis 1), would perceive more suspicion towards them when interviewed with a suspicion-oriented interview protocol (Hypothesis 2), and would provide more information when interviewed with a suspicion-oriented interview protocol (Hypothesis 3). Finally, it was theorised that actualisers would experience a need to secure successful implementation of a threat. Hence, it was predicted that actualisers would be more reluctant to share implementation details than bluffers (i.e. how-related information; Hypothesis 4). The manuscript of Study II was published in the *Journal of Applied Research in Memory and Cognition* (see Appendix F).

Method

Participants and design

A total of 195 participants, mainly undergraduate university students at the University of Gothenburg (Sweden), took part in the study (134 women, 46 men, 15 missing; $M_{age} = 26.60$ years, $SD = 7.38$ years) in which they made a threat via a phone call. They participated on a voluntary basis and received a movie ticket worth approximately €12 in return. Fifteen participants did not make the call because they (a) felt uncomfortable doing so ($n = 13$), (b) had participated in a similar study before ($n = 1$), or (c) due to a technical failure ($n = 1$). Their data were excluded from further analysis. Hence, a sample of 179 participants remained (130 women, 46 men, 3 other; $M_{age} = 26.60$ years, $SD = 7.35$ years). Participants were randomly assigned as bluffers ($n = 90$) or actualisers ($n = 89$). Furthermore, a random half of the bluffers and actualisers were assigned to be questioned with the high-suspicion protocol ($n = 91$), and the other half were assigned to be questioned with the low-suspicion protocol ($n = 88$).

Procedure

The procedure largely resembled the threat paradigm developed for Study I. Participants were presented with a case that reflected a moral conflict between a fictive Non-

Governmental Organisation (NGO) named Aweare and a fictive clothing company named Vera. Participants read how Aweare was dedicated to improving working conditions in low-wage countries and how Vera was known as being socially engaged in the local communities in the countries where Vera outsourced their production. Vera had recently released a commercial in which they drew attention to violence against women. Meanwhile, Aweare got hold of video recordings showing how Vera exploited women in factories in Cambodia. Aweare considered it hypocritical for Vera to raise public awareness about violence against women while simultaneously exploiting them for their own profit. Aweare therefore decided to take action against Vera. Participants were instructed to imagine being part of Aweare and to represent Aweare in this action.

All participants were instructed to call a representative of Vera. They were instructed to threaten to leak the video recordings containing evidence of Vera's malpractice to the media, unless the company withdrew their commercial from television. Participants were either instructed to bluff when making this claim and thus not truly leak the recordings (bluffers), or to do as they claimed and leak the recordings right after the call, regardless of the outcome of the call (actualisers). All participants were given 15 minutes to prepare for their task(s) and all had access to the same background materials (e.g. information about Aweare, working conditions in Cambodia, route to the delivery location for the recordings). Participants were allowed to make notes and to have those with them while talking to Vera.

Next, the participants phoned the representative of Vera. The recipient of the call was a confederate who responded to the threats according to structured interview protocols, displayed in Table 3. Each participant was initially invited to speak freely (free-statement phase) and was then questioned about the threat he or she made (specific-questions phase). Half of the participants were asked high-suspicion questions/prompts, suggesting that the interviewer aimed to assess the truthfulness of the threat (high-suspicion protocol; e.g. "How do I know that what you are saying is true?"). The other half were asked low-suspicion questions/prompts, suggesting that the interviewer aimed to better understand the threat (low-suspicion protocol; e.g. "To make sure that I get you right, I need to know more").

After the call, the experimenter informed all participants that the Vera representative thought they were bluffing and therefore decided to ignore the threat. They were then instructed to proceed with their task according to the instructions. Bluffers were supposed to do nothing, whereas actualisers were supposed to provide their media contact with a USB stick containing the video recordings. They were intercepted immediately after starting the implementation (e.g. when walking towards the door).

Each participant was then asked to answer closed and open-ended questions about the strategies they had used in their communication with Vera. They were asked whether or not they had used any particular strategy (if so, to describe this strategy) and whether they had changed their strategy during the call (if so, to explain why). Next, each participant completed the perceived suspicion scale by rating three items; "Vera believed me", "Vera trusted me", and "Vera was suspicious of me" (1 = *not at all*; 7 = *very much*; Buller, Strzyzewski, & Comstock, 1991; $\alpha = .68$). To compute an overall measure of perceived suspicion, the average score on the three items was calculated after reversing two on the three items (belief, trust) so that a higher score on the items reflected a higher level of perceived suspicion. Each participant further rated nine statements related to their involvement in the case (e.g. "It is important that action is taken against Vera"; $\alpha = .74$), their belief in the authenticity of the case, how difficult they had found the instructions and their task, how nervous they had been for their task, how sufficient the time for preparation had been, and how willing they had been to give Vera information.

Table 3

Interview Protocols That Were Used to Answer the Participants' Threat Calls

Free-statement phase	
Hello, my name is Caroline. I'm the head of public relations at Vera's and I expected your call. You initiated this conversation, so please go ahead.	
Specific-questions phase	
Low-suspicion protocol	High-suspicion protocol
The reason that I take this call is because it is my responsibility <i>to understand you correctly</i> . Therefore I would like to ask you to provide me with more information.	The reason that I take this call is because it is my responsibility <i>to find out whether or not you are telling the truth</i> . Therefore I would like to ask you to provide me with more information.
Thank you. But this is not yet enough for me <i>to draw the entire picture. To complete my task and make sure that I get you right, I need to know more.</i>	Thank you. But this is not yet enough for me <i>to make a proper judgement. How do I know that what you are saying is true?</i>
Before we finish this conversation, is there anything else that <i>I should know of?</i>	Before we finish this conversation, is there anything else that <i>could further convince me?</i>

Note: Italics indicate words that differed between the interview protocols.

All scales ranged from 1 (*not at all*) to 7 (*very much*). Participants were then thoroughly debriefed, thanked for their participation, and handed the movie ticket as reward for participation.

Coding

Provided information. Two trained coders coded the transcribed calls. Each transcript was coded for (a) the total amount of information revealed, which was further broken down into the amount of (b) ‘why’ and (c) ‘how’ information, reflecting Vallacher and Wegner’s (1987) distinction between ‘why’ aspects (why to threaten) and ‘how’ aspects of an action (how to enact the threat). The same coding scheme as in Study I was used. The scheme included 76 pieces of information in the background materials to which the participants had access while preparing for the call. Of this total, 44 pieces were classified as ‘why’ information, and 32 pieces were classified as ‘how’ information. For instance, explanations about the poor conditions in Cambodia, the malpractice of Vera, or the vision of Aweare were classified as ‘why’ information. Moreover, details such as the delivery location or the name of the media contact were classified as ‘how’ information. Each transcript was coded for new pieces of information. A piece of information was considered new when it was mentioned for the first time by the participant. Repetitions were thus not taken into account. Two coders coded 20% of the transcripts, resulting in agreement on 92% of the decisions made (Cohen’s $\kappa = .77$). One of the coders completed the remaining 80% of the transcripts. The coders were blind to the condition of the participants and the hypotheses of the study.

Reported strategies. Two coders coded the answers provided for the strategy question (i.e. “Describe the strategy you used during your communication with Vera”). Reported strategies were divided into two categories, mirroring the previously described ‘how’ versus ‘why’ division. Strategies focused on the implementation of the threat were classified as ‘how’ strategies (e.g. “My strategy was to convince Vera that I really had the material, and that giving it to my contact would be problematic for them”). Strategies focused on motivating the threat were classified as ‘why’ strategies (e.g. “I tried to make Vera realise that their business operation is hypocritical”). When participants reported both type of strategies, only the main strategy was coded (e.g. the following statement was coded as a ‘how’ strategy, “My strategy was to show my power by stressing that I had the USB stick in my hand. I also tried to be informative”). When both types of strategies were equally prevalent, it was coded as “both” (e.g. “I tried to make clear that their vision went against the actual working conditions. I pointed

out that I had proof and was ready to reveal the proof to the public”). Strategies that fitted neither one of the two categories were classified as “other”. After the coders coded 20% of the answers and reached an interrater agreement of 86% (Cohen’s $\kappa = .70$), one coder proceeded with the remaining material. Again, the coders were unaware of the conditions and hypotheses.

Change of strategies. The open-ended question on strategy change (i.e. “Explain why you changed strategy during the communication with Vera”) was included for exploratory purposes. Hence, a data-driven scheme was used to code the participants’ answers, meaning that one individual, blind to the conditions, used the answers to identify broader categories in the data. Four reasons for strategy change were identified: (1) The participant did not get the response that they had wanted/expected, (2) the participant was asked to provide more information, (3) the participant was asked to prove their point, and/or (4) the conversation was coming to an end. It was possible for participants to report more than one reason. Reasons that fitted neither one of the four mentioned categories were classified as ‘other’. Two individuals coded 20% of the material. After calculating the interrater agreement (93%, Cohen’s $\kappa = .73$), one coder completed the remaining material.

To reiterate, the experimental design involved suspects making a threatening phone call to a company. The threat was about leaking a video containing evidence of malpractice. The phone call included two sections; a free report section initiated by the threatener, followed by a series of prompts initiated by the company. Manipulations were made with respect to the instructions to the threateners (“bluff about the threat” vs. “actualise the threat”) and with respect to the level of suspicion raised by the company in the prompts (high vs. low). The dependent variables were i) the amount of (‘how’ and ‘why’) information provided in each section of the threat statement, ii) the self-reported strategies used to present the case, and iii) the self-reported reasons for strategy change.

Results

Manipulation checks

The descriptive statistics of the participants’ self-ratings are displayed in Table 4. The table reveals that participants assessed the case as authentic, rated high involvement with Aware’s case against Vera, understood the instructions, and reported that they had sufficient time to prepare for their tasks. Yet, participants found their tasks demanding and were nervous about completing them. This was true for both making the threat call and for delivering the USB stick (the latter was rated by actualisers only). Independent t-tests showed that none of

Table 4

Mean Values (and Standard Deviations) of Bluffers' and Actualisers' Involvement with the Case, Experienced Difficulty to Comply with the Instructions, and Nervousness about Performing the Tasks

Rating	Bluffer	Actualiser
Involvement with case	5.52 (0.77)	5.66 (0.77)
Belief that case rested on authentic facts	5.69 (1.36)	5.94 (1.04)
Understanding of instructions	5.92 (1.03)	5.89 (1.12)
Sufficiency of preparation time	4.81 (1.79)	4.31 (1.80)
Difficulty making call	4.82 (1.51)	4.67 (1.75)
Difficulty preparing delivery	N/A	2.86 (1.62)
Nervousness about making call	5.13 (1.65)	5.28 (1.69)
Nervousness about delivering	N/A	2.94 (1.87)

Note: There were no significant differences between bluffers and actualisers on the reported ratings ($p > .05$). All ratings were made on 7-point Likert scales (1 = *not at all*, 7 = *very much*).

these measures differed significantly between actualisers and bluffers, all t 's (177) < 1.81 , p 's $> .07$.

Actualisers and bluffers were supposed to have different intentions with regard to delivering the USB stick. Actualisers were supposed to deliver the stick immediately after making the threat call, whereas bluffers were not. To check if all participants acted accordingly, the experimenter waited for the participants to initiate or not initiate the first move towards delivery (e.g. walking towards the door). All actualisers started the implementation, whereas none of the bluffers did. Hence, the manipulation of intent was considered successful.

Perceived suspicion

A 2 (Threat: bluff vs. actualise) \times 2 (Protocol: high suspicion vs. low suspicion) between-subjects ANOVA on the level of perceived suspicion, revealed a main effect of protocol, $F(1, 175) = 11.53$, $p = .001$, $\eta_p^2 = .06$. The participants who were questioned with the high-suspicion protocol reported to have experienced more suspicion directed towards them

($M = 5.44$, $SD = 1.00$) than the participants questioned with the low-suspicion protocol ($M = 4.93$, $SD = 1.03$), which supports the effectiveness of the protocols. Note that both protocols induced suspicion awareness, and the low-suspicion protocol thus refers to *lower* (rather than low) suspicion induction compared to the high-suspicion protocol. Furthermore, there was no main effect of threat, $F(1, 175) = 2.90$, $p = .090$, $\eta_p^2 = .02$. In contrast to Hypothesis 2, no significant interaction was found between Threat and Protocol, $F(1, 175) = 0.83$, $p = .364$, $\eta_p^2 = .01$. Bluffers and actualisers experienced similar levels of suspicion in the low-suspicion protocol ($M_{\text{bluff}} = 4.73$, $SD = 1.00$; $M_{\text{actualise}} = 5.13$, $SD = 1.03$), as well as in the high-suspicion protocol ($M_{\text{bluff}} = 5.38$, $SD = 1.07$; $M_{\text{actualise}} = 5.50$, $SD = 0.92$). Thus, the highly suspicious questions affected bluffers' and actualisers' perceived suspicion to the same extent.

Provided information

It was found that all participants were fairly forthcoming in the free-statement phase. About half of the total amount of information given by bluffers and actualisers was provided during the free-statement phase (bluffers 47%, actualisers 54%). This finding was further supported by the participants' self-rated willingness to share information, showing that both bluffers ($M = 5.02$, $SD = 1.57$) and actualisers ($M = 5.40$, $SD = 1.39$) were rather willing to share information, $t(177) = -1.72$, $p = .086$, $d = .26$, 95% CI [-.551, .038]. The willingness rating was significantly related to the actual amount of information provided in the interview, $r = .20$, 95% CI [.059, .353], $p = .008$.

To test the hypotheses with regard to information provision (H1, H3, and H4), three separate ANOVA's were conducted. The descriptive statistics of all three analyses are displayed in Table 5. First, a 2 (Threat: bluff vs. actualise) \times 2 (Phase: free-statement vs. specific-questions) mixed ANOVA was performed on the total amount of details provided in the statements, with Threat as the between-subjects factor, and Phase as the within-subjects factor. The analysis revealed no main effects of Threat, $F(1, 177) = 0.66$, $p = .419$, $\eta_p^2 = .00$, or Phase, $F(1, 177) = 0.00$, $p = .983$, $\eta_p^2 = .00$. However, there was a significant Threat \times Phase interaction effect, $F(1, 177) = 4.19$, $p = .042$, $\eta_p^2 = .02$. Tests of simple effects provided support for Hypothesis 1. As can be seen in Figure 1a, bluffers provided more information in the specific-question phase than actualisers did, $F(1, 177) = 4.74$, $p = .031$, $\eta_p^2 = .03$, whereas no such difference was found for the free-statement phase, $F(1, 177) = 1.58$, $p = .211$, $\eta_p^2 = .01$.

Second, to test the influence of suspicion, a 2 (Threat: bluff vs. actualise) \times 2 (Protocol: high suspicion vs. low suspicion) between-subjects ANOVA was conducted on the information provided in the specific-question phase. Already reported, bluffers provided more information

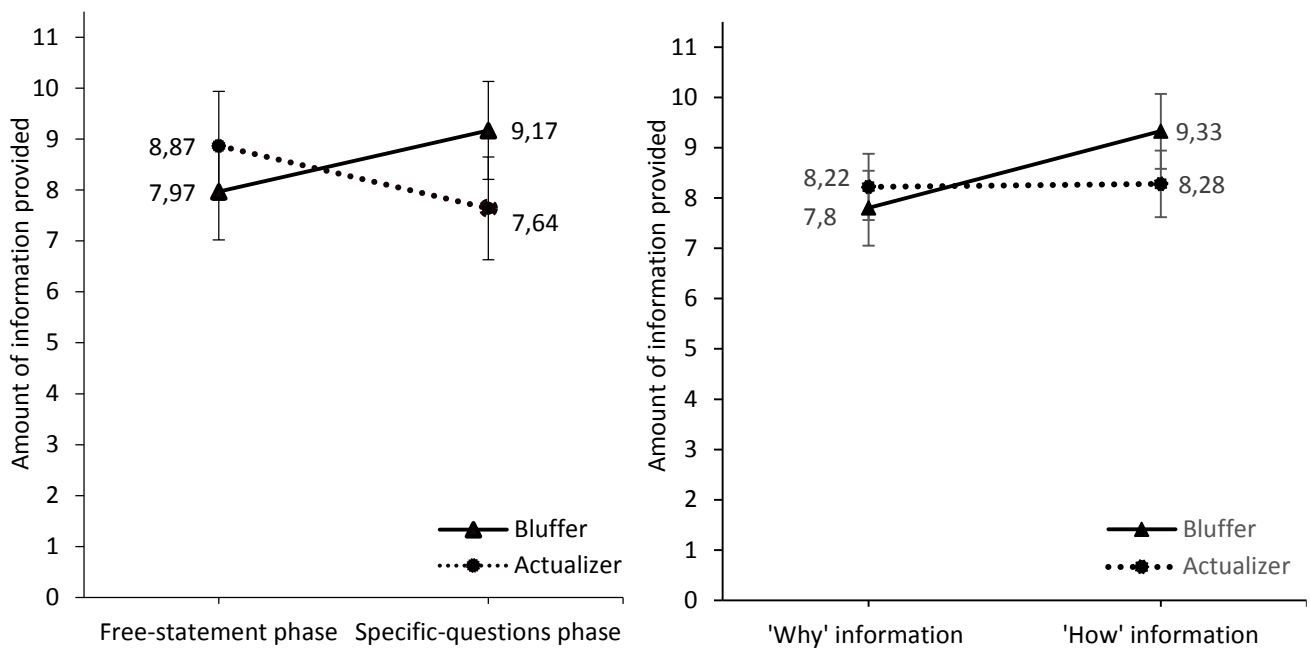
Table 5

Mean values (and Standard Deviations) for the Amount of Information that Bluffers and Actualiser Provided in their Threat Statements by Phase, Protocol, and Information

	Free-statement phase	Specific-questions phase
Threat	<i>M (SD)</i>	<i>M (SD)</i>
Bluffer	7.97 (4.52)	9.17 (4.60)a
Actualiser	8.87 (5.04)	7.64 (4.78)
	Low-suspicion protocol	High-suspicion protocol
Threat	<i>M (SD)</i>	<i>M (SD)</i>
Bluffer	9.84 (4.78)	8.52 (4.37)
Actualiser	7.11 (4.93)	8.16 (4.62)
	‘How’ information	‘Why’ information
Threat	<i>M (SD)</i>	<i>M (SD)</i>
Bluffer	9.33 (3.56)	7.80 (3.53)
Actualiser	8.28 (3.33)	8.22 (3.13)

in the specific-question phase compared to actualisers, hence a significant main effect of Threat was found, $F(1, 175) = 4.89, p = .028, \eta_p^2 = .03$. There was no main effect for Protocol, $F(1, 175) = 4.89, p = .028, \eta_p^2 = .03$. Importantly, no support was found for Hypothesis 3. The mean values even suggest an opposite trend. That is, bluffers provided more information than actualisers when questioned under low suspicion (rather than under high suspicion), but this Threat \times Protocol interaction was not found statistically significant, $F(1, 175) = 2.85, p = .093, \eta_p^2 = .02$.

Third, a 2 (Threat: bluff vs. actualise) \times 2 (Information: how vs. why) mixed ANOVA was performed to examine the type of information provided by bluffers and actualisers. No main effect of Threat was found, $F(1, 177) = 0.66, p = .419, \eta_p^2 = .00$. However, the analysis revealed a main effect of Information $F(1, 177) = 5.86, p = .017, \eta_p^2 = .03$, showing that participants revealed more ‘how’ than ‘why’ information. There was a significant Threat \times Information interaction, $F(1, 177) = 5.06, p = .026, \eta_p^2 = .03$. In support of Hypothesis 4, simple effect tests revealed that bluffers provided significantly more ‘how’ details throughout their



Note. Error bars denote 95% confidence intervals

Figure 1a. Total amount of information provided by bluffers and actualisers in the free-statement phase and in the specific-questions phase.

Figure 1b. Amount of 'why' and 'how' information provided by bluffers and actualisers.

statement than did actualisers, $F(1, 177) = 4.14$, $p = .043$, $\eta_p^2 = .02$, whereas no significant difference between the groups was found for the amount of 'why' details provided, $F(1, 177) = 0.73$, $p = .396$, $\eta_p^2 = .00$. This effect is displayed in Figure 1b.

Strategies

Nearly all participants reported to have used some strategy when communicating the threat (94%). The vast majority of the reported strategies (78%) could be classified as a 'how' (35%), 'why' (35%) or 'both' (8%). Chi-square analyses revealed that bluffers and actualisers reported to have used 'how' and 'why' strategies to an equal extent (see Table 6). Hence, the findings on reported strategies lend no further support to Hypothesis 4. Further, participants were asked if they changed their strategies during the conversation, and if so, why they changed strategy. Out of 164 participants who reported to have had a strategy, 82 (50%) reported to have changed strategy during the conversation. Participants reported to have changed strategy (a)

Table 6

Reported Strategies by Bluffers and Actualisers

Strategy	Bluffers	Actualisers	X^2	p	ϕ
Why (focus on explaining the threat)	29 (32%)	33 (37%)	0.47	.495	.05
How (focus on implementing the threat)	32 (36%)	31 (35%)	0.01	.919	.01
Both ('how'/'why' to an equal extent)	5 (6%)	9 (10%)	1.29	.256	.08
Other	16 (18%)	13 (15%)	0.33	.565	.04
No strategy	8 (9%)	3 (3%)	2.36	.124	.11

because the response from Vera differed from what they had wanted/expected (42%; e.g. “When I noticed a lack of moral response, I tried to instill fear”), (b) because they were asked to provide more information (29%; e.g. “When I suddenly was asked to clarify my point, I tried to explain how they violate human rights”), (c) because they were asked to prove their point (17%; e.g. “When Vera wanted me to show that I was telling the truth, I tried to rethink and express myself differently”), (d) because the end of the conversation was approaching (10%; e.g. “Towards the end, when Vera did not sound convinced, I tried to push more towards the fact that it was in their own interest”), and/or (e) for other reasons (6%; e.g. “I lost what I was going to say and strayed away from my strategy”). Seven participants (9%) did not report the reason for their change of strategy. Chi-square analysis revealed no significant differences between bluffers and actualisers for the number of strategy changes or for the type of reasons reported ($X^2 < 3.84$).

An explorative analysis was conducted to examine the influence of suspicion on the number of strategy changes reported. A chi-square analysis showed that a comparable percentage of participants interviewed under low suspicion (43.4%) and high suspicion (56.8%) made strategy changes, $X^2(1, N = 164) = 2.95, p = .086, \phi = .13$.

In addition, the relationship between strategy change and information provision was further explored in a mixed Change (yes vs. no) \times Phase (free-statement vs. specific-questions) ANOVA on the amount of information provided. Note that only the participants who reported to have used a strategy were included in the analysis ($n = 164$). The analysis yielded a near-significant Change \times Phase interaction, $F(1, 162) = 3.64, p = .058, \eta_p^2 = .02$. The trend in the data points out that participants who reported a shift in strategy, increased their information

provision from the free-statement phase ($M = 7.96$, $SD = 4.91$) to the specific-question phase ($M = 8.96$, $SD = 4.99$), whereas participants who reported no shift in strategy decreased their information provision from the free-statement phase ($M = 8.93$, $SD = 4.67$) to the specific-question phase ($M = 7.54$, $SD = 4.49$).

Last, the correlation was tested between type of strategies reported (how vs. why) and type of information provided (how vs. why). A positive correlation was found between the reported use of 'why' strategies and the amount of 'why' information provided, $r_{pb} = .338$, $p < .001$. No correlation was found between the reported use of 'how' strategies and the provision of 'how' information, $r_{pb} = .072$, $p = .422$.

Gender

Female participants ($M = 5.67$, $SD = 0.73$) reported a significantly higher involvement with the case, compared to male participants ($M = 5.34$, $SD = 0.85$), $t(174) = 2.527$, $p = .012$, $d = .50$, 95% CI [.16, .84]. Gender differences were also found for the moment of information disclosure. Female participants provided significantly more information in the free-statement phase ($M = 8.84$, $SD = 4.86$) than male participants did ($M = 7.17$, $SD = 4.51$), $t(174) = 2.038$, $p = .043$, $d = .35$, 95% CI [.01, .69], but male participants provided significantly more information in the specific-question phase ($M = 9.96$, $SD = 4.82$) than female participants did ($M = 7.96$, $SD = 4.62$), $t(174) = 2.615$, $p = .010$, $d = .45$, 95% CI [.11, .79]. However, these gender differences were not found to interact with the manipulations of the study. Thus, male and females responded similarly to the threat-manipulations (bluff vs. actualise) and to the interview-manipulation (low vs. high suspicion protocol), all p 's $> .309$. No gender differences were found for the amount of how-information provided ($p = .749$), the amount of why-information provided ($p = .681$), or for the reported use of strategies ($p = .292$).

Discussion

Nearly all participants reported to have used a strategy when communicating their threats. Strategies focusing on implementation of the threat (how-related strategies) were reported as often as strategies focusing on motivation for the threat (why-related strategies). Half of all participants who reported to have used a strategy changed strategies during the interaction in order to successfully withstand questioning. Bluffers and actualisers did not differ in their strategy use. Moreover, participants reported to be fairly willing to share information with the interviewer and spontaneously provided about half of the total amount of information to which they had access (i.e. in their free-statement). Thus, while participants were found to

be forthcoming, they were also strategic and adaptive to the target's responses. These findings suggest that threateners avail of self-regulative mechanisms when being questioned about their intent regardless of whether they are bluffing or not—a suggestion that matches theory and research on self-presentation which states that both guilty and innocent suspects must regulate their behaviour (albeit in different ways) in order to make a credible impression (DePaulo, 1992; Hartwig et al., 2010).

The hypotheses were partly confirmed. Actualisers provided fewer details concerning the implementation of the threat than did bluffers (supporting H4). This finding replicated the results of Study I. Furthermore, bluffers provided more information in response to specific-questions as compared to actualisers (supporting H1). However, this difference was not increased by the use of a suspicion-oriented interview protocol (rejecting H3). The latter result is probably best explained by the finding that bluffers and actualisers reported to have experienced similar levels of suspicion (rejecting H2). Thus, communicating suspicion in the interview had no particular impact on bluffers. The study did not provide a clear explanation for this particular finding, yet, the finding differs from research showing that lying interviewees (which bluffers can be considered to be) are more sensitive to the risk for not being believed (Hartwig et al., 2010; Vrij, Fisher, Mann, & Leal, 2008).

With regard to gender, it was found that female (vs. male) participants were more involved with the case, and provided more information in their free statement (but comparatively less information in response to the interviewer's questions). One explanation for these differences might be that females related more to the content of the case (i.e., violations of women rights) compared to males. Importantly, the gender differences were found to exist independent of the manipulations in the study. For instance, whether they were bluffing or actualising, females were more informative than males in their free statement. Moreover, whether they were interviewed under low or high-suspicion, males were more informative than females in response to questions. Thus, there existed some gender differences in involvement and responsiveness but these differences did not impact the main findings of the study.

Although the predicted differences between bluffers and actualisers were partly confirmed, the current study did not provide a clear insight into the processes explaining these differences. Some possible mediators were not explicitly measured (e.g., that actualisers find implementation details risky to reveal; that bluffers are more concerned about their credibility), and others could not be properly established (e.g., that bluffers perceive more suspicion directed towards them; that actualisers intentionally conceal 'how' details). A more general shortcoming is that the student sample used may speak against the external validity of the study. It can be

argued that the average student differs from the average person who poses a threat of violence. Finally, the magnitudes of the differences found between bluffers and actualisers were small to moderate. Small differences may be valuable on a theoretical level, as these could tell something about underlying mechanisms that are at play, but on an operational level it is unlikely that small behavioral differences can be detected by professionals who interact with subjects of concern.

Study III

It could be argued that skilled interviewing starts with an understanding of the interviewee's perspective (Granahag & Hartwig, 2008). Therefore, Study III advanced Study II by exploring what types of counter-interview strategies threateners employ. In addition, the study examined the efficacy of two interview approaches commonly used in law enforcement and intelligence gathering contexts: *direct interviewing* vs. *rapport-based interviewing* (Alison, et al., 2013; Justice et al., 2010). It was predicted that rapport-based interviewing would be more effective for threat assessment and management purposes (Bull, 2013; Meissner et al., 2014). Specifically, it was predicted that threateners interviewed with the rapport-based protocol would use fewer counter-interview strategies (Hypothesis 1), provide more information (Hypothesis 2), display a lower willingness to carry out a threat (Hypothesis 3), and display a higher willingness to interact (meet) with the conflicting party again (Hypothesis 4) than threateners interviewed with the direct protocol. The manuscript of Study III was submitted for publication to the *Journal of Psychology, Crime, and Law* (see Appendix G).

Method

Participants and Design

One hundred and twenty students at the University of Gothenburg (33 men, 83 women, 4 other, $M_{age} = 27.38$ years, $SD = 8.83$ years) participated in the experiment on a voluntary basis. The gender category "other" consisted of participants who categorized themselves as neither man nor woman. Participation took approximately 40 minutes and participants were compensated with 100 SEK (approx. 11 USD). Participants were randomly assigned to one of two interview conditions: direct interviewing ($n = 60$) or rapport-based interviewing ($n = 60$).

Procedure

Participants were recruited for a study on ‘career challenges’. Upon arrival, they read a fictitious case about a work conflict between a consultancy company and a former employee. The case file revealed how the company had allegedly tricked recent graduates into unpaid internships by promising them a permanent position. After the internship, however, their contract was ended and the company had profited from free labour. A duped employee wrote a letter to the company in which s/he threatened to press charges against this malpractice, unless the company would financially compensate her/him for the work carried out. Participants were asked to imagine being this employee. See Appendix A for the full background story and the instructions to the participants.

First, participants were asked to list up to five reasons for why they would press charges at this point in time, as well as reasons for why they would *not* press charges at this point in time. This task was meant to stimulate the participants to think carefully about the case before they rated four items about their *willingness to enact the threat* (i.e. to press charges). Participants rated the extent to which (i) they believed they could win the case in a court of law, (ii) they thought the case was worth pursuing, even if it would be rather expensive, (iii) they thought the case was worth pursuing even if it would take time, and (iv) they were likely to press charges (1 = *not at all*, 9 = *very much*; $\alpha = .85$). The procedure was repeated for the participants’ *willingness to interact* with the company about their case; participants were first asked to list reasons for and against interacting with them at this point in time, and then rated the extent to which (i) they would be willing to communicate with the company if the company would contact them about their case, (ii) they would seek contact with the company to provide the company with information about their case, and (iii) they would seek contact with the company to gather information about their case (1 = *not at all*, 9 = *very much*; $\alpha = .64$).

Next, participants were informed that an employee of the internal security unit from the company would discuss the case with them. Participants were then given 10 minutes to prepare themselves for this meeting and they received additional information about their case (e.g. an overview of the hours they had worked for the company, the contact details of a counsellor). Participants were allowed to make notes and to bring those with them to the meeting. Furthermore, participants were told to keep in mind that “If you reveal too much, the company might take advantage of the information you provide. If you reveal too little, the company might not take you seriously”. This was supposed to reflect the information-management dilemma that interviewees in the legal arena typically face (Hartwig et al., 2010; Granhag et al., 2016).

Immediately after the preparation phase, participants were brought to the meeting room. The role of the interviewer was played by one of two confederates (man and woman) who were

blind to the hypotheses of the study. The interviewers conducted an equal number of interviews across conditions. All participants received the same 11 questions/prompts. The questions tapped into topics that are considered to be relevant in threat management (e.g. motivation, intentions, capacity; Vossekuil et al., 2015). Half of the participants were approached with a *direct interview protocol*, meaning that the questions/prompts were asked straightforwardly. The other half were approached with a *rapport-based interview protocol*, meaning that the questions/prompts were phrased in a rapport-promoting manner. The interview protocols are displayed in Appendix B.

After the interview, participants rated the same seven items as they had rated before the interview, about their willingness to enact the threat at this point in time (four items, $\alpha = .89$), and about their willingness to interact with the company in the future (three items, $\alpha = .73$). In addition, the participants were asked to report if they had used a particular strategy when interacting with the interviewer (and if so, to describe this strategy). Finally, participants reported their age, gender, and current occupation.

Protocol Pretesting

The interview protocols were pretested in a separate study. A total of 141 participants (80 men, 61 women) judged to what extent the interview protocols were rapport-promoting. Participants were recruited from Amazon's Mechanical Turk and they were each compensated 0.50 USD. Participants were randomly assigned to one of two interview protocols; the direct interview protocol ($n = 73$) or the rapport-based interview protocol ($n = 68$). First, participants read the fictitious case about the work conflict between the consultancy company and the former employee (see Appendix A) so that they would understand the context of the interview questions. Next, they listened to the interview questions as if they were the interviewee. Finally, participants rated 13 items reflecting elements of rapport (e.g. 'The interviewer understands the difficult situation that I am in', see for all items Appendix C). The items were rated on a 7-point Likert scale (1 = *strongly disagree*, 7 = *strongly agree*; $\alpha = .83$).

In support of the design, participants exposed to the rapport-based interview protocol reported significantly higher ratings of rapport ($M = 4.05$, $SD = 0.79$) than participants exposed to the direct interview protocol ($M = 3.55$, $SD = 0.96$), $t(139) = 3.43$, $p < .001$, $d = 0.58$, 95% CI [0.24, 0.91].

Coding

Strategy use. The strategies that the participants reported to have used were divided into six categories; *prove capability*, *conceal*, *self-presentation*, *explain*, *negotiate*, and *other*. Two categories, *conceal* and *self-presentation*, were drawn from previous research in the counter-interview strategies of suspects (Hartwig et al., 2010) and two categories, *prove capability* and *explain*, were drawn from previous research into counter-interview strategies of threateners (Geurts et al., 2016). The category *negotiate* was added because of the business-like nature of the case (i.e. work conflict, financial request). Strategies that did not fit any of these five categories were coded as *other*. The participants could report more than one strategy. Two coders, both blind to the hypotheses of the study, categorised the strategies. Based on 20% of the material, an interrater agreement of 87% was established (Cohen's $\kappa = .65$). After settling the disagreements, one coder coded the remaining material.

Information provision. All interviews were transcribed and coded for the amount and type of information disclosed. The background story given to the participants consisted of 45 pieces of information (see Appendix A). These information pieces suited the interview questions (see Appendix B). That is, the participants could use the background information to answer the questions that they were about to receive. For instance, the information piece 'You kept track of your working hours while working for the company' could be used to answer the question 'Why do you think that your case is a strong case?' Again, two coders, unaware of the hypotheses, separately coded 20% of the material. The coders counted which information pieces were present in each transcript and reached an interrater agreement of 89% (Cohen's $\kappa = .73$). One coder continued coding the rest of the material.

Results

Hypotheses Testing

Strategy use. Nearly all participants ($n = 108$, 90%) reported to have used a strategy during the interview. Almost half of them ($n = 49$, 45.4%) reported a single strategy, while the majority ($N = 59$, 55.6%) stated to have used a combination of two to four different strategies. As can be seen in Table 7, the most frequently reported strategies were *prove capability* ('Show them that my evidence would hold in court') and *conceal* ('Answer as vaguely as possible'). Other reported strategies were *self-presentation* ('Appear professional and credible'), *explain*

Table 7

Frequencies of Threateners' Self-Reported Counter-Interview Strategies

Strategy	Total	Interview protocol		χ^2
		Direct	Rapport	
Prove capability	59 (49.2%)	34 (56.7%)	25 (41.7%)	2.70
Conceal	56 (46.7%)	32 (53.3%)	24 (40.0%)	2.14
Self-presentation	27 (22.5%)	9 (15.0%)	18 (30.0%)	3.87
Explain	21 (17.5%)	8 (13.3%)	13 (21.7%)	1.44
Negotiate	9 (7.5%)	5 (8.3%)	4 (6.7%)	0.12
Other	18 (15.0%)	10 (16.7%)	8 (13.3%)	0.26
No strategy	12 (10.0%)	6 (10.0%)	6 (10.0%)	0.00

Note. Threateners could report more than one strategy; thus, percentages do not add up to 100%. The χ^2 values refer to the difference between the direct and rapport-based interview conditions in the proportion of participants who reported the strategy. None of these tests were statistically significant at $p < .05$ (Bonferroni corrected).

(‘Make them understand my difficult situation’), negotiate (‘Show willingness to reach an agreement’), and other (‘Take over control by asking questions back’). The two strategies that were most often used in combination were prove capacity and conceal ($n = 32$).

The number of participants who claimed to have used a strategy was the same across interview conditions ($n = 54$ [90%] in both conditions). Chi-square tests did not reveal any significant differences in the extent to which participants in the rapport-based interview condition and the direct interview condition reported to have used the different type of strategies, all $ps < .343$ (Bonferroni corrected). Thus, there was no effect of interview protocol on reported strategy use, meaning that Hypothesis 1 was not supported.

Information provision. Participants were found to be moderately forthcoming, with an average disclosure of 12.74 ($SD = 4.67$) information pieces per person out of the total of 45 pieces (i.e. 28.3%). An independent t -test revealed that participants in the rapport-based interview condition ($M = 13.45$, $SD = 4.93$) and direct interview condition ($M = 12.05$, $SD =$

4.37) did not differ significantly with respect to the amount of information provided, $t(118) = 1.63$, $p = .106$, $d = 0.30$, 95% CI [-0.06, 0.66]. This means that Hypothesis 2 is rejected.

Willingness to enact. To test the effect of the interview on willingness to enact the threat, a 2 (Protocol: direct vs. rapport-based) \times 2 (Time: before interview vs. after interview) mixed ANOVA was performed with participants' willingness ratings as the dependent measure. Cell means are reported in Table 8. No main effect of protocol was found, $F(1, 118) = 0.69$, $p = .407$, $\eta_p^2 = 0.006$, 90% CI [.000, .048]. However, the analysis revealed a main effect of Time, $F(1, 118) = 12.79$, $p < .001$, $\eta_p^2 = .098$, 90% CI [.029, .187], indicating that participants were significantly more willing to enact the threat after ($M = 6.35$, $SD = 1.81$) than before the interview ($M = 5.84$, $SD = 1.76$). There was no significant Protocol \times Time interaction, $F(1, 118) = 1.42$, $p = .236$, $\eta_p^2 = .012$, 90% CI [.000, .063]. Thus, the amount of change between before- and after-interview ratings did not differ significantly between the two interview protocols, rejecting Hypothesis 3.

Willingness to interact. To test the effect of the type of interview on participants' willingness to interact with the company, a 2 (Protocol) \times 2 (Time) mixed ANOVA was performed (for cell means, see Table 8). No main effect of interview protocol was found, $F(1, 118) = 0.07$, $p = .794$, $\eta_p^2 = .001$, 90% CI [.000, .024]. However, the analysis again revealed a main effect of time, $F(1, 118) = 30.06$, $p < .001$, $\eta_p^2 = .203$, 90% CI [.104, .303], showing that participants were significantly less willing to interact with the company after ($M = 5.29$, $SD = 2.10$) than before the interview ($M = 6.16$, $SD = 1.78$). There was no significant Protocol \times Time interaction, $F(1, 118) = 2.39$, $p = .626$, $\eta_p^2 = .020$, 90% CI [.000, .078]. Thus, the rate of

Table 8

Means of Before- and After-Interview Ratings as a Function of Interview Protocol

Interview protocol	Willingness to enact		Willingness to interact	
	Before	After	Before	After
Direct	5.87 (1.74)	6.56 (1.68)	6.24 (1.81)	5.29 (2.14)
Rapport	5.80 (1.79)	6.15 (1.93)	6.08 (1.75)	5.28 (2.08)

Note. Both *willingness to enact* and *willingness to interact* were rated on 9-point Likert scales. Values in parentheses represent standard deviations.

decline of willingness to interact with the company did not differ between the two interview protocols, rejecting Hypothesis 4.

Exploratory Analyses

The main analyses were conducted for the overall amount of information provided. However, from an applied perspective, some information might be more critical than other information. Hence, 12 raters were asked to read the case and to select the 8 to 12 (out of 45) pieces of information that they considered to be the most critical for assessing the risk that the main character in the case would cause harm. An independent *t*-test was conducted with the information pieces that were selected by five or more raters ($n = 15$). On average, participants revealed 5.80 ($SD = 2.19$) out of 15 pieces of this critical information. No significant difference was found between participants in the rapport-based interview condition ($M = 6.07$, $SD = 2.36$) and participants in the direct interview condition ($M = 5.53$, $SD = 2.67$), $t(118) = 1.16$, $p = .248$, $d = 0.21$, 95% CI [-0.15, 0.57].

To examine whether strategy choice influenced the amount and type of information provided, independent *t*-tests were conducted with respect to the two most frequently reported strategies—*prove capability* and *conceal*. First, participants with the strategy *prove capability* did not provide a significantly different amount of detail on the implementation of the threat ($M = 4.39$, $SD = 2.94$) than did participants who did not employ this particular strategy ($M = 3.85$, $SD = 2.57$), $t(118) = 1.07$, $p = .288$, $d = 0.19$, 95% CI [-0.16, 0.55]. Second, the participants who reported to have used the strategy *conceal* provided on average about two details less ($M = 11.64$, $SD = 5.12$) than did participants who did not use this particular strategy ($M = 13.70$, $SD = 4.09$), $t(118) = 2.45$, $p = .016$, $d = 0.45$, 95% CI [0.09, 0.81].

In total, 56 participants reported to have used the strategy *conceal*. Some of these participants ($n = 33$) were vague in their descriptions about what information they withheld (e.g. ‘I left out the important details’), whereas others ($n = 23$) specified which type of information they concealed. The latter group reported to have concealed three types of information: (i) information about persons that could help them implement the threat (e.g. the names of a potential witness, companion, or legal counsellor; $n = 19$), (ii) information about their own vulnerability (e.g. emotional or financial problems; $n = 7$), and (iii) specific pieces of evidence (e.g. documentation that proved their argument; $n = 5$). Participants could report to have concealed more than one type of information.

Moreover, the participants who reported to have used the strategy *conceal* were found to be significantly more willing to enact the threat before the interview ($M = 6.29$, $SD = 1.60$) than were the participants who did not report to have used this particular strategy ($M = 5.44$, $SD = 1.81$), $t(118) = 2.69$, $p = .008$, $d = 0.49$, 95% CI [0.13, 0.86]. This finding might imply that those with more serious implementation intentions more often chose to conceal information. However, no correlation was found between willingness to enact the threat and the amount of information provided, $r = .069$, $p = .455$, 95% CI [-.112, .245].

Finally, we examined to what extent participants' initial attitudes toward enacting the threat and attitudes toward interacting with the conflicting party (before-interview ratings) correlated with their attitudes after the interview. Positive correlations were found between before- and after-interview ratings for willingness to enact the threat, $r = .604$, $p < .001$, 95% CI [.476, .707], and willingness to interact with the conflicting party, $r = .609$, $p < .001$, 95% CI [.482, .711]. In a similar vein, only 21 participants (17.5%) changed the direction of their willingness to enact the threat ($n = 7$ willing to unwilling; $n = 14$ unwilling to willing) after the interview compared to before, and only 29 (24.2%) of the participants changed the direction of their willingness to interact with the conflicting party ($n = 23$ willing to unwilling; $n = 6$ unwilling to willing). A change in direction was counted when participants rated an average value greater than 5 (on a 9-point Likert scale) before the interview, and an average value lower than 5 after the interview—and vice versa. Two 3 (Change: unwilling to willing; willing to unwilling; no directional change) \times 2 (Protocol: direct vs. rapport-based) chi-square tests revealed no significant differences between interview conditions for the number of participants that changed the direction of their willingness to enact the threat, $\chi^2(2, N = 120) = 0.52$, $p = .771$, $\phi = .07$, or to interact with the conflicting party, $\chi^2(2, N = 120) = 0.05$, $p = .973$, $\phi = .02$.

No correlation was found between the participants' willingness to enact the threat and their willingness to interact with the conflicting party. This result was true for the before-interview ratings ($r = -.106$, $p = .249$) as well as for the after-interview ratings ($r = -.054$, $p = .559$).

Discussion

Replicating the findings of Study II, threateners were found to be semi-cooperative when questioned about their harmful intentions. They were willing to discuss their case and provided, on average, one third of the information held (and approximately 40% of the critical information held), but most of them (90%) were also strategic in presenting their case. The most frequently reported strategies were to *prove capability* ("Show them that my evidence would

hold in court”) and *conceal* (“Answer as vaguely as possible”). These findings imply that threateners use a mix of forthcoming and withholding strategies attempting to strike a deliberate balance between proving their standpoint and concealing details.

Contrary to expectations, no differences were found between interview protocols for participants’ strategy use (rejecting H1), information provision (rejecting H2), or willingness to carry out the threat (rejecting H3) or discuss the case (rejecting H4). These outcomes stand in contrast to previous research supporting the efficacy of rapport-based interviewing over accusatorial or direct interviewing (Bull, 2013; Meissner et al., 2014). Two possible explanations for the null results are proposed. First, the rapport-promoting elements in the rapport-based interview protocol may have been too weak, implying that more profound means are needed to steer the interviewees’ behaviour. The pilot study revealed that the rapport-based interview protocol was perceived as significantly more rapport-promoting than the direct interview protocol, but these ratings did not differ much in absolute terms (i.e., the rapport-based and direct protocols received average ratings of 4.05 and 3.55 on a 7-point scale, respectively). Moreover, an average score of 4.05 on a 7-point scale suggests that the rapport-based protocol was rapport-promoting only to a moderate extent. Second, the case scenario reflected an economic argument which may have been too rational (rather than emotional) in nature. It has been suggested that rational (or instrumental) crises with a typical win-lose structure are best confronted with logical arguments as opposed to rapport-building approaches (Giebels & Taylor, 2010).

Exploratory analyses revealed that interviewing had an escalating rather than deescalating effect, regardless of the interview protocol. Specifically, threateners were more willing to carry out the threat after the interview than before and were also less willing to interact with the conflicting party after the interview than before. Furthermore, initial attitudes of the threateners were found to be predictive of post-interview attitudes. Those who were relatively more eager to carry out the threat or interact with the conflicting party from the start were also relatively more eager to do so after the interview. Importantly, participants initially more positive towards carrying out the threat chose to conceal information more often, especially information concerning the actual implementation of the threat (e.g. names of contact persons, specific pieces of evidence). This finding suggests that threateners with serious intent to strike may employ more avoidant strategies than bluffers.

Study IV

Study IV was an online study with threat assessment professionals and non-professionals. The study investigated whether threat assessments made by professionals were of higher quality than those made by non-professionals. Based on research on expert performance, quality was defined by the ability to perform consistently (as compared with peers) and base decisions on relevant information (Dror, 2016; Einhorn, 1974). Specifically, it was predicted that professionals would agree more with one another with respect to risk assessments as compared to non-professionals (Hypothesis 1) and that professionals' search for information would be comparatively more in line with empirically supported threat cues (Hypothesis 2). Threat cues were defined as pieces of information that indicate an increased risk for violence. The manuscript of Study IV was published in the *Journal of Investigative Psychology and Offender Profiling* (see Appendix G).

Method

Participants and Design

A total of 141 participants completed the survey. The sample consisted of 45 assessment professionals (30 men, 15 women, $M_{age} = 44.87$ years, $SD = 10.13$ years), 46 university students (12 men, 34 women, $M_{age} = 27.42$ years, $SD = 9.97$ years), and 50 laypersons (19 men, 31 women, $M_{age} = 42.48$ years, $SD = 13.01$ years). The sample size was guided by the number of professionals that could be recruited, meaning that the number of students and laypersons was matched with the number of professionals that participated. The reason for including two non-professional samples (students and laypersons) was that students may not fully represent the non-professional population, as they are studying to become professionals of some kind themselves. Working experience in threat assessment averaged 12.70 years ($SD = 8.96$) in the professional sample. One participant in the professional sample reported to have just one year of working experience in threat assessment and seven participants in the non-professional samples reported to have more than one year of working experience in threat assessment. The data of these eight individuals were excluded from further analyses. One hundred and thirty-three participants remained, of whom 44 were professionals (30 men, 14 women, $M_{age} = 45.23$ years, $SD = 9.95$ years), 44 were students (12 men, 32 women, $M_{age} = 26.53$ years, $SD = 8.63$ years), and 45 were laypersons (17 men, 28 women, $M_{age} = 42.09$ years, $SD = 12.80$ years)¹.

¹ Gender and age, when included as covariates in statistical analyses, did not change the pattern of the results and will be disregarded in the reported analyses.

Professionals were approached via associations of threat assessment professionals in Europe (Association of European Threat Assessment Professionals, AETAP) and in Canada (Canadian Association of Threat Assessment Professionals, CATAP) to take part in a survey on threat assessment. They were either members of these associations, attended a conference on threat assessment in April 2016 that was organised by AETAP, or they were recommended as eligible participants by those who were initially approached. The countries in which the professionals operated were Canada ($n = 9$), The Netherlands ($n = 8$), Germany ($n = 7$), the United States ($n = 3$), Australia ($n = 3$), worldwide ($n = 3$), Austria, Belgium, Hong Kong, Luxembourg, New Zealand, South-Africa, Sweden, and Switzerland (all $n \leq 2$). Professionals were not financially rewarded for their participation.

Students and laypersons were recruited for a study about how people make risk judgments. Students were approached via the participant pool of the University of Gothenburg (Sweden) where they had signed up for participation in psychological research. They were each compensated 50 SEK (approx. 6 USD). Laypersons were approached online through Amazon's Mechanical Turk (MTurk) and were each paid 0.50 USD upon completion. Participants in the laypersons sample were from the United States ($n = 41$) and India ($n = 9$). All participants completed the same survey. The data collection took place from April to June 2016.

Materials

Three fictitious cases were constructed in which a person posed a potential threat of violence towards one or several other persons. To prevent the outcomes from being the result of one particular case or one particular domain of violence, each case reflected a different domain of violence that is commonly encountered in the field of threat assessment. These domains were intimate partner violence (case "Terry"), public figure violence (case "Marc"), and workplace violence (case "Frank"). Case Terry described a domestic conflict in which a man, Terry, poses a potential threat towards his ex-girlfriend for breaking up with him. Case Marc described a case in which a university student in chemistry, Marc, poses a potential threat towards the Minister of Health and Social Affairs, as Marc holds him responsible for colluding with corrupt parties in the pharmaceutical industry. Case Frank describes a work conflict in which an employee, Frank, utters a written threat towards his employer and colleagues after he was informed that he might lose his job due to forced redundancies.

Each case consisted of 15 to 21 information cues describing i) the context in which the threat evolved and ii) the behaviours and characteristics of the person posing the threat. Each information cue in the cases was selected based on risk factors and protective factors that have

been found to be empirically valid. For instance, the information cue *Frank's position within the firm is uncertain* reflected the risk factor “employment instability” (Feldman & Johnson, 1996). Protective factors are conditions and behaviours that may reduce the risk of violence, which can also be the absence of risk factors (Borum, 2000). For instance, the information cue *Frank joins a running group twice a week* indicated the absence of the risk factor “social isolation” (Meloy, White, & Hart, 2013). In addition to the risk and protective factors, each case held two pieces of neutral information. That is, information that is not empirically known to increase or decrease the risk for violence as such (e.g. having tattoos). Two experienced threat assessment professionals provided feedback on the cases. They read the case scenarios (see Appendix H) and judged the cases to be similar to those they would encounter in their profession, and hence, perceived the storylines as relevant and realistic.

Procedure

The first page of the survey stated that the study included three descriptions of separate cases in which a person poses a potential threat. The participants were instructed to read each case and to answer the accompanying questions. Participants were informed that participating was confidential, voluntary, and for research purposes only. After agreeing on these terms, they were presented with the first case, followed by three questions. First, participants were asked to assess the overall risk for physical violence currently posed by the main character (0% = *no risk for violence*, 100% = *guaranteed risk for violence*; any number between 0 and 100 could be selected). Next, they were presented with a list of specific information cues derived from the case. They were asked to assess the extent to which each information cue increased or decreased the risk for violence in this particular case (e.g. *Frank's position within the firm is uncertain*; -4 = *very strong decrease*, 0 = *neutral*, 4 = *very strong increase*). Finally, participants were asked to list up to five additional information cues that they would request in order to make a more adequate assessment of the risk for violence for this particular case. The same procedure was repeated for each case. The cases were presented in a randomised order.

After completing the case-related questions, participants provided their age, gender, and number of years working in the field of threat assessment. In addition, professionals were asked to indicate in which country they worked and how they were professionally involved in threat assessment (e.g. screening and security, criminal intelligence gathering). Students and laypersons were asked to indicate their country of residence and their employment status (e.g. student, employed for wages). Participants needed approximately 30 minutes to complete the survey.

Data Analyses

Coding. Two research assistants coded the information cues requested by the participants. First, the total number of requested information cues was counted per participant per case (ranging from 1 to 5). Second, each information request was classified as ‘*key request*’ or ‘*other request*’. A request was considered a ‘key request’ when it matched one of the 11 key questions identified by Vossekuil, Fein, and Berglund (2015). These key questions are supposed to cover all areas that should be inquired in order to make a fully informed assessment about a person posing a threat. Information requests that did not fit any of the key questions were categorised as ‘other request’. The ‘other requests’ were then further qualified into specific areas of inquiry. All areas of inquiry specifying ‘key requests’ and ‘other requests’ are listed in Table 9. Two coders categorised a random 30% of the material into ‘key requests’ vs. ‘other

Table 9

Areas of Inquiry Used to Classify Requested Information

Key requests (Vossekuil et al., 2015)
<ol style="list-style-type: none"> 1. What are the subject’s motives and goals? 2. What has the subject communicated about his or her intentions to anyone (target, law enforcement, family, friends, colleagues, associates, diary/journal)? 3. Is there evidence that the subject has engaged in attack-related behaviours? 4. Is there evidence that the subject has engaged in menacing, harassing, and/or stalking type behaviour? 5. Does the subject have a history of mental illness involving command hallucinations, delusional ideas, feelings of persecution, and so forth, with indications that the subject has acted on those beliefs? 6. How organised is the subject? Does the subject have the ability to plan and execute a violent action? 7. Is there evidence that the subject is experiencing feelings of hopelessness, desperation, or despair? 8. Is what the subject says consistent with his or her actions? 9. Does the subject see violence as acceptable, desirable, or the only way to solve problems? 10. What concerns do those who know the subject have about the subject’s behaviour? 11. What factors in the subject’s life and/or environment could change and thereby increase the subject’s risk of attacking? What factors could change and thereby decrease the risk posed?
Other requests
<ol style="list-style-type: none"> 1. Requests about upbringing 2. Requests about criminal records that do not concern violence or stalking 3. Requests about drugs, alcohol and medication that do not concern mental illness 4. Requests about protective factors that do not concern the future 5. Requests about finances without a specified reason for the request 6. Requests that do not fit any of the previous categories

requests' (85.71%, Cohen's $\kappa = .71$) and further specified the requests into one of 17 specific areas of inquiry (74.44%, Cohen's $\kappa = .66$). One coder completed codings on the remaining material.

Results

Initial Analysis of Risk Assessments

To reiterate, the assignment of a risk value (1 = *very strong decrease*, 9 = *very strong increase*) to one information cue was considered one assessment. The three cases together contained 57 information cues. Hence, each participant made 57 assessments of specific information cues. One-sample *t*-tests revealed that professionals assessed information cues that reflected risk factors as risk increasing (i.e. the average rating was significantly higher than the neutral value "5"; $M_{\text{professional}} = 6.44$, $SD = 0.56$, $t(43) = 17.14$, $p < .001$, $d = 5.17$), and information cues that reflected protective factors as risk decreasing (i.e. the average rating was significantly lower than the neutral value "5"; $M_{\text{professional}} = 3.90$, $SD = 0.74$, $t(43) = 9.93$, $p < .001$, $d = 2.99$). Information cues that reflected neither risk factors nor protective factors were rated as neutral (i.e. the average rating was statistically similar to the neutral value "5"; $M_{\text{professional}} = 4.97$, $SD = 0.48$, $t(43) = 0.45$, $p < .652$, $d = 0.14$). Students and laypersons made ratings similar to those of professionals for risk factors ($M_{\text{student}} = 6.31$, $SD = 0.56$, $t(43) = 15.37$, $p < .001$, $d = 4.63$; $M_{\text{layperson}} = 6.05$, $SD = 0.98$, $t(44) = 7.18$, $p < .001$, $d = 2.14$) and for protective factors ($M_{\text{student}} = 4.16$, $SD = 1.06$, $t(43) = 5.27$, $p < .001$, $d = 1.59$; $M_{\text{layperson}} = 3.86$, $SD = 1.25$, $t(44) = 6.01$, $p < .001$, $d = 1.79$). However, the neutral cues were rated as neutral by laypersons ($M_{\text{layperson}} = 4.72$, $SD = 1.27$, $t(44) = 1.44$, $p = .156$, $d = 0.43$), but as risk decreasing by students ($M_{\text{student}} = 4.49$, $SD = 1.34$, $t(43) = 2.56$, $p = .014$, $d = 0.78$).

The mean values for each information cue are displayed in Figure 2. As shown in the figure, the professionals' assessments were highly similar to the assessments of the non-professionals. Only two out of 57 information cues were assessed in one direction by professionals (risk decrease) and in the other direction by non-professionals (neutral / risk increase). Although this could have been the result of chance, the two items (*Rebecca has avoided all contact with Terry*; *Rebecca has received a new telephone number and moved to another neighbourhood*) reflected a similar theme, which was, contact between victim and threatener in partner violence. Furthermore, participants in all three samples assigned the highest risk values to information cues that reflected a communicated threat.

Besides assessing specific information cues, participants were asked to judge the *overall* risk for violence for each case (0% = *no risk*, 100% = *guaranteed risk*). A 3 (Sample:

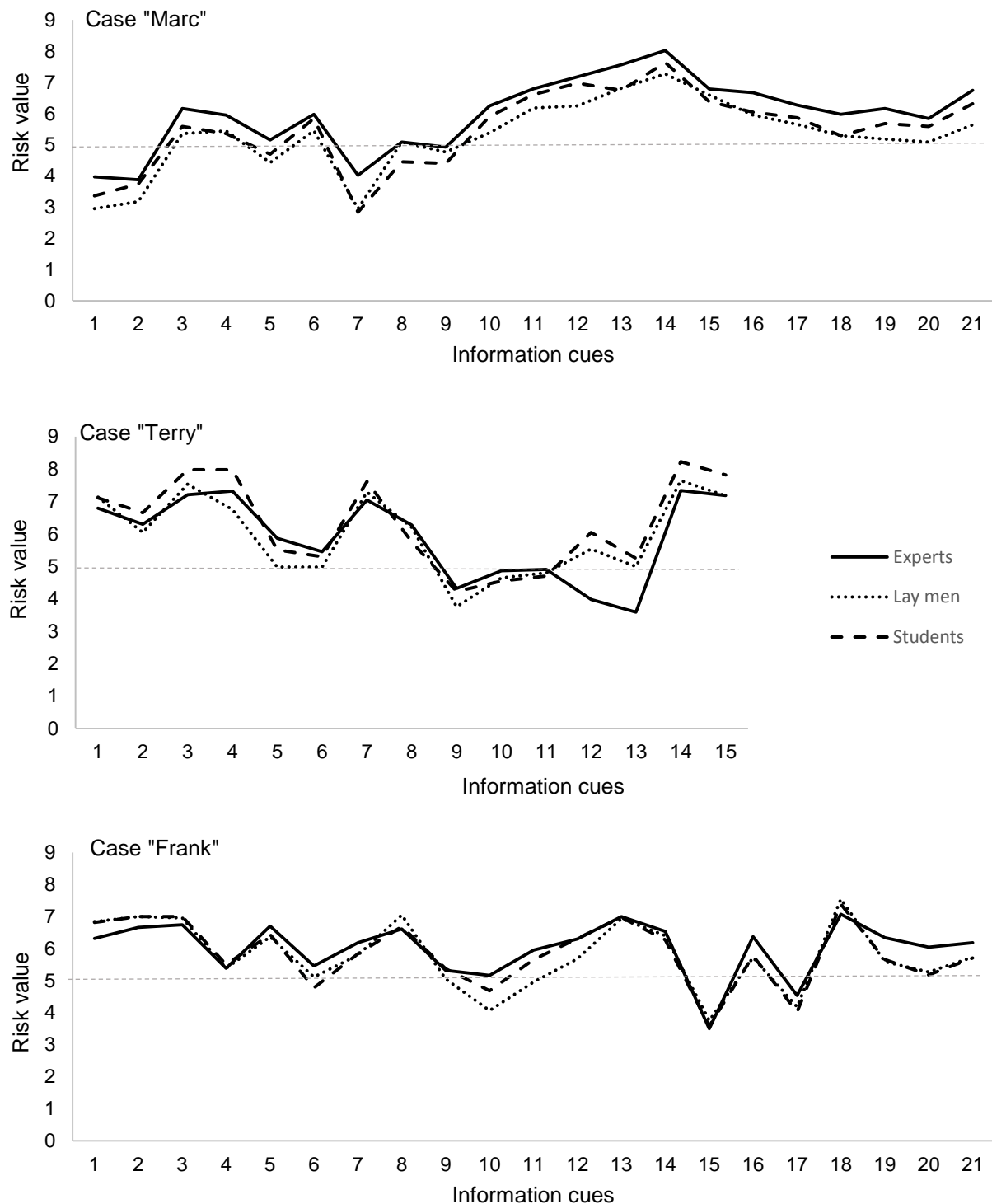


Figure 2. Risk assessments (1 = *very strong risk decrease*, 9 = *very strong risk increase*) that professionals, students, and laypersons made for the information cues presented per case.

Table 10

Mean Percentages for Violence Risk per Case Judged by Professionals, Students, and Laypersons

	Professionals	Students	Laypersons
Case “Marc”	43.05% (20.17)	46.11% (20.75)	43.56% (24.54)
Case “Terry”	57.83% (23.84)	76.07% (17.29)	71.98% (17.53)
Case “Frank”	48.62% (23.87)	47.73% (22.25)	55.44% (20.89)

Note. Mean percentages are based on a rating scale ranging from 0% (*no risk for violence*) to 100% (*guaranteed risk for violence*). The numbers in parentheses represent standard deviations.

professionals vs. students vs. laypersons) \times 3 (Case: Terry vs. Marc vs. Frank) mixed ANOVA was performed on the violent risk ratings, with Sample as the between-subjects factor. The descriptive statistics are reported in Table 10. The analysis showed no significant main effect of Sample, $F(2, 128) = 3.04, p = .05, \eta_p^2 = .05$, but there was a significant main effect of Case, $F(2, 128) = 61.51, p < .001, \eta_p^2 = .33$. Participants judged the risk for violence in case “Terry” significantly higher than in case “Frank”, $F(1, 128) = 55.84, p < .001, \eta_p^2 = .30$, and they judged the risk in case “Frank” significantly higher than in case “Marc”, $F(1, 128) = 8.90, p < .01, \eta_p^2 = .06$. Furthermore, the analysis yielded a significant Sample \times Case interaction effect, $F(4, 256) = 4.01, p = .004, \eta_p^2 = .06$. Tests of simple effects revealed different risk assessments across samples for case “Terry”, $F(2, 128) = 10.09, p < .001, \eta_p^2 = .14$. Professionals judged the overall risk for violence lower than did students ($p < .001$) and laypersons ($p = .001$). No difference was found between students and laypersons ($p = .329$). Furthermore, no differences across samples were found for case “Mark”, $F(2, 128) = 0.24, p = .784, \eta_p^2 = .04$, or for the case “Frank”, $F(2, 128) = 1.59, p = .208, \eta_p^2 = .02$.

Hypothesis Testing

Agreement. Agreement among assessors becomes apparent in the standard deviation of their ratings, with the lower the standard deviation, the more similar the ratings. A 3 (Sample: professionals vs. students vs. laypersons) \times 3 (Case: Terry vs. Marc vs. Frank) between-items ANOVA was conducted on the standard deviations for the information cues. A main effect for Sample occurred, $F(2, 162) = 106.67, p < .001, \eta_p^2 = .568$. Planned contrasts showed that the average standard deviation within the professional sample ($M = 1.14, SD = 0.21$) was

significantly lower than the average standard deviation within the student sample ($M = 1.48$, $SD = 0.26$, $p < .001$) and the layperson sample ($M = 1.75$, $SD = 0.91$, $p < .001$). Post hoc tests further revealed that the difference between the student sample and the layperson sample was significant ($p < .001$). The main effect of Case was not statically significant, $F(2, 162) = 0.52$, $p = .598$, $\eta_p^2 = .006$, neither was the Sample x Case interaction effect, $F(4, 162) = 1.51$, $p = .200$, $\eta_p^2 = .036$. Thus, the results indicate that the consensus among the professionals was systematically (i.e. regardless of the case) higher than the consensus among the non-professionals. This supports Hypothesis 1.

The above analysis does not account for where on the 9-point scale the spread was located. Spread on the lower (1-3), central (4-6), or higher part (7-9) of the scale was weighted equally. However, when examining agreement using this scale, the spread on the central part may be particularly relevant because it contains both a risk decreasing value (4) and a risk increasing value (6). More specific, agreement on the *direction of risk* (i.e. increase or decrease) can be considered more critical than agreement on the magnitude of risk (e.g. strong increase or very strong increase). To test for differences between samples in agreement on direction, a chi-square test was performed on the number of confidence intervals within each sample that included the central value of the scale ("5"). Confidence intervals containing the middle value imply that some participants in the sample rated the information as risk decreasing (values below 5), whereas others in the sample rated the same information as risk increasing (values above 5). The six neutral information cues were excluded from the analysis because these cues were expected to obtain ratings close to the value of 5. The analysis was conducted on the assessments of the remaining 51 information cues. A significant difference across samples was found with regard to the number of confidence intervals containing the value 5, $\chi^2(2, N = 153) = 8.70$, $p = .013$, $\phi = .24$. In further support of Hypothesis 1, professionals rarely disagreed with each other on whether information should be assessed as risk increasing or risk decreasing ($N = 3$, 5.9%), whereas such disagreement among laypersons occurred in approximately one third of the assessments made ($N = 14$, 27.5%, $p < .05$). The frequency of disagreement among students ($N = 8$, 15.7%) was not found to be significantly different from the other two samples.

Information search. After assessing the risk for violence, participants were asked to list up to five additional information cues that they considered relevant for making a more adequate assessment. The requested information cues were classified into 'key requests' and 'other requests', and further divided into different areas of inquiry (see the Method section). ANOVA's were conducted for each case on (a) the total number of information requests, (b)

Table 11

Means and Inferential Statistics for the Analyses of the Requested Information

Measure	Professionals	Students	Laypersons	<i>F</i>	<i>p</i>	η_p^2
Case "Marc"						
No. of information pieces requested	3.66 (1.55)	2.16 (1.60)	2.56 (1.67)	10.27	.000	.136
'key requests'	2.68 (1.63)	1.18 (1.08)	1.62 (1.13)	15.42	.000	.192
'other requests'	0.98 (1.00)	0.95 (1.18)	0.93 (1.23)	0.02	.984	.000
No. of areas inquired	3.23 (1.46)	1.86 (1.31)	2.13 (1.34)	12.24	.000	.158
Case "Terry"						
No. of information pieces requested	3.91 (1.54)	2.11 (1.70)	2.51 (1.53)	14.68	.000	.185
'key requests'	2.64 (1.63)	1.07 (1.19)	1.22 (0.97)	22.70	.000	.260
'other requests'	1.27 (1.11)	1.05 (1.16)	1.29 (1.49)	0.25	.779	.004
No. of areas inquired	2.95 (1.40)	1.64 (1.33)	1.91 (1.02)	12.46	.000	.162
Case "Frank"						
No. of information pieces requested	3.82 (1.72)	2.27 (1.48)	2.49 (1.62)	11.93	.000	.155
'key requests'	2.64 (1.54)	1.34 (1.12)	1.56 (1.16)	12.84	.000	.165
'other requests'	1.18 (1.24)	0.98 (1.30)	0.93 (1.16)	0.51	.602	.008
No. of areas inquired	3.11 (1.56)	2.00 (1.24)	2.09 (1.26)	9.15	.000	.123

Note. The numbers in parentheses represent standard deviations.

the number of 'key requests', (c) the number of 'other requests', and (d) the number of different areas that were inquired. The latter measure served as an indication for the variety of the requested information. Descriptive and inferential statistics are presented in Table 11. Planned contrasts confirmed Hypothesis 2. Professionals requested significantly more key information than students (all cases $p < .001$) and laypersons (all cases $p < .001$). Furthermore, requests that were made by professionals covered significantly more different areas of inquiry compared to requests made by students (all cases $p < .001$) or laypersons (all cases $p \leq .001$). Post-hoc tests showed no differences between students and laypersons on any of the measures. Thus, when

given the opportunity to gather additional data, professionals requested comparatively more relevant information and from a comparatively wider variety of domains.

Discussion

The results demonstrated support for both hypotheses. A higher level of consensus was found among professionals than among students and laypersons (supporting H1). Moreover, the professionals requested comparatively more relevant information (i.e. key requests) and their requests covered a wider range of topics (supporting H2). These findings held true in all three cases. Both measures (inter-rater agreement and empirically supported decision-making) reflect quality standards in expert performance (Dror, 2016; Einhorn, 1974). Hence, the results suggest that domain-specific experience adds to the quality of threat assessment practices. That said, risk assessments were found to be strikingly similar across all three groups. Professionals' beliefs of which cues were (and were not) alarming were very similar to those of non-professionals. This finding suggests that actual assessment of information in threat cases may, in part, reflect common sense.

The results of Study IV fit neatly with previous research on expertise and risk perception in which professionals were found to excel at cue selection (i.e. what information should be looked for) (Elstein & Schwarz, 2002; Fahsing & Ask, 2016) but not assumed (Slovic & Weber, 2002) or found to be better at cue assessment (i.e. how the information should be interpreted; Bogaard, Meijer, Vrij, & Merckelbach, 2016). In brief, threat assessment professionals may contribute most to the process of gathering (rather than assessing) information.

One shortcoming of the study was that it did not tap into the participants' reasoning behind their assessments. Therefore, it remains unknown if (and if so, how) participants connected the information cues to possible risk factors. For instance, suffering from diabetes was included as a neutral factor since diabetes has never been proven to relate to the enactment of threats. However, a participant could have reasoned that suffering from a chronic disease is a stressful condition and should thus be assessed as information that is risk increasing. Such reasoning would be in line with research showing that personal stressors may indeed indicate a higher risk for violence (Meloy et al., 2013). Another potential concern is that the cues in the cases may have been self-evident, meaning that their interpretation was straightforward. For example, the cue Marc is highly frustrated that the Minister has not replied. It is quite clear that frustration is risk increasing rather than risk decreasing. If the information given was less ambiguous than the information threat assessors typically face in real life, this may form an alternative explanation for the similarities found between the professionals and non-

professionals. A final note is warranted on a possible bias in the professional sample. Professionals may have been more motivated than non-professionals as the study concerned their own field of expertise. This could explain the higher number of information requests on behalf of the professionals.

CHAPTER 3: GENERAL DISCUSSION

The aim of this thesis is to contribute to a scientific approach for threat assessment and management (TAM) interviewing. It is important that threat assessment professionals, to the fullest extent possible, engage with persons who pose a threat because only *they* hold first-hand information of their intentions and only *they* can change their intentions. While TAM interviewing has long been acknowledged and practiced, the topic has been ignored in research. This thesis is one of the first attempts to fill that gap. An experimental paradigm was developed to examine interview dynamics in a threat assessment context. The paradigm was tested and used in a series of studies, each addressing the topic from a slightly different angle. The first two studies were developed from a deception detection perspective. Specifically, is it possible to elicit verbal cues to deceit in threat statements (Study I) and can one interview strategically to create verbal cues to deceit in threat statements (Study II)? In the follow-up studies, there was a shift of perspective from deception detection towards risk assessment and information gathering. Specifically, what interview approach contributes most to information gathering and de-escalation in threat cases (Study III) and do threat assessment professionals gather and assess information in threat cases differently to non-professionals (Study IV)? Irrespective of the research angle (deception detection or information gathering), it is argued throughout the thesis that it is vital for TAM interviewers to understand what attitudes and behaviours can be expected from the threatener. Counter-interview strategies were therefore explored in both Studies II and III.

Main Findings

Avoidant Actualisers

The most consistent outcome of the laboratory studies was that persons more likely to carry out the threat were found to be less informative about its implementation. In Studies I and II, the likelihood of carrying out the threat was manipulated by assigning participants to either bluff about the threat (bluffers) or actualise the threat (actualisers). Actualisers in both studies disclosed fewer details than bluffers regarding how they would carry out the threat. In Study III, it was found that persons who reported to be more willing to carry out the threat more often reported to have concealed information as part of their strategy. In particular, they reported to have withheld information that could aid the implementation of the threat, such as contact

details of accomplices. In all three lab-studies, bluffers and actualisers were found to be equally informative on a general level when explaining their case and their motivation for threatening.

These findings are neither in line with the experience of professionals, nor theory and research in cognitive psychology. For instance, according to the FBI's National Center for the Analysis of Violent Crimes (NCAVC), the more detailed a threat is, the more serious the risk for actual implementation (O'Toole, 2009). Their reasoning parallels the Construal Level Theory (CLT) holding that the specifics of an event dominate people's minds if the event is likely to occur (Trope & Liberman, 2010). Supporting the CLT, previous research has shown that people tend to give detailed accounts describing events they believe to be likely to happen (Wakslak et al., 2006) or when describing actions they truly intend to carry out (Mac Giolla, et al., 2013; Mac Giolla & Granhag, 2015; Sooniste et al., 2014; 2015).

Despite being based on evidence and logic, the CLT was not supported in the present studies on threat assessment. This outcome might be best explained in the light of self-regulation (Fiske & Macrae, 2012). Concretely, the mind-set of actualisers might be detailed and implementation-oriented, but, to prevent others from interfering with their plans, actualisers must conceal critical details from the conflicting party. Avoidant regulation strategies (e.g. keeping the story simple, avoiding lies) have been found to be particularly common in interrogations with guilty suspects who have a need to conceal criminal involvement (Hartwig et al., 2007; Strömwall et al., 2006). In threat cases, critical details are most likely to be about the implementation of the threat (i.e. how-related details). For instance, an actualiser who leaks the time or location of the planned attack allows authorities to arrange for extra security measures. Moreover, revealing the names of accomplices could hinder successful implementation and challenge social bonds. Thus, actualisers maintain a critical advantage by concealing information from the interviewer.

Practically, the present findings imply that detailed threat accounts should not automatically be interpreted as cause for concern. Yet, suggesting the opposite ("He is elaborating on the implementation of the threat so he is probably bluffing") would be taking a step too far. For starters, the studies within this thesis did not directly test the diagnostic value of implementation details in threat statements. Furthermore, previous studies that did examine the ability to distinguish between statements of true and false intent revealed error rates of approximately 30% (Vrij et al., 2011a, b). Such error rates are unacceptable when assessing the risk for violence in real cases. Perhaps, the most important conclusion to be drawn here is that threateners treat information about their case strategically when being questioned; they choose what information to reveal and conceal. This notion is valuable for TAM interviewers because

a strategic approach from the interviewee allows for, or even requires, a strategic approach from the interviewer. This topic will be discussed in more depth in the next section.

Semi-Cooperative Interviewees

Threateners' counter-interview strategies were examined in two of the three laboratory studies (II and III). Threateners in both studies were found to be semi-cooperative interviewees. On one hand, threateners were willing to interact and share information with the interviewer, they truly provided a fair amount of information (25-30% of all the information they held), and no one refused to speak. On the other hand, nearly all threateners (90-94%) reported to have approached the interview strategically. Semi-cooperative attitudes were also revealed in the type of strategies participants reported to have used. Forthcoming strategies (e.g. "I wanted to show them that my evidence against them is strong") were often combined with withholding strategies (e.g. "I tried to answer as vaguely as possible").

In brief, the findings support the self-regulation perspective which states that people tend to control their behaviour in social settings in order to reach desired outcomes (Fiske & Macrae, 2012). Self-regulation is assumed to be of particular significance in challenging social interactions. Examples of challenging social interactions are those in which a person must conceal the truth to protect matters of personal relevance (e.g. freedom, money, opportunities) and those in which the integrity of a person is openly questioned. Since both of these aspects are typically part of interrogation situations, the self-regulation perspective provides a relevant theoretical framework for research on how to interview suspects (DePaulo, 1992; Hartwig et al., 2010).

Drawing a parallel between previous studies on suspect interviewing and the current findings, two things are notable. First, reported strategy use in the current studies is much higher than that from research on suspect interviewing. Hartwig and colleagues (2007) found that 60% of guilty suspects and 37% of innocent suspects reported to have had a strategy before the interrogation. An explanation for the high rates among threateners may be that they perceive the burden of explanation to rest on themselves. In contrast, suspects are involuntarily taken in for questioning which automatically places suspects in a comparatively more reactive position ("Let's see what they have on me"). Second, the participants making threats seemed to combine a typical innocent-suspect attitude (being forthcoming; Strömwall et al., 2006) with a typical guilty-suspect attitude (being strategic; Hartwig et al., 2007). This combination might result from the fact that the difference between morally right (i.e. being innocent, telling the truth) and morally wrong (i.e. being guilty, telling a lie) is less clear when stating a threat. Bluffers

have no intention to commit harm, but they are guilty of lying about their intentions (i.e. innocent liars). Actualisers intend to commit harm, but they are honest in their claim (i.e. guilty truth-tellers). Taken together, both threat interviewing and suspect interviewing represent challenging interactions that require self-regulation by the interviewee. Yet, the act of threatening clearly differs from a suspect giving a statement and this could explain the unique patterns found in the current studies.

The finding of forthcoming threateners fits well with professional reports that threateners are typically willing to discuss their case (van der Meer & Diekhuis, 2014; White, 2014). However, the finding that threateners can be strategic in TAM interactions is rarely mentioned in the literature, with the exception of Meloy and Mohandie (2014) who note that persons posing a terror threat may use countermeasures to undermine the interview. The strategic aspect is an important addition. Being aware of counter-strategy use is the first step towards altering and exploiting it.

Persistent Interviewees

Studies II and III examined the efficacy of different interview styles but none of those examined led to significant differences in the interviewees' behaviours or attitudes. Suspicion-oriented interviewing did not result in differences between the statements of bluffers and actualisers (Study II). Moreover, rapport-based and direct interviewing evoked similar responses in terms of the threateners' strategy use, information provision, and willingness to pursue or discuss the threat (Study III). These outcomes deviate from research supporting the efficacy of rapport-based interviewing over accusatorial or direct interviewing (Bull, 2013; Meissner et al., 2014), as well as from theory and research demonstrating that guilty and innocent suspects respond differently to the risk of not being believed (Hartwig et al., 2010).

The lack of impact from different interview styles may be explained by methodological shortcomings. The manipulation of perceived suspicion levels and rapport might not have been powerful enough or, perhaps, suspicion levels and rapport are not critical to TAM interviews. In other words, more intense manipulation or other independent variables might have been more influential (see also Limitations). An alternative explanation could be that threateners are particularly steadfast interviewees. Two of the current findings support this argument. The first is the frequent use of counter-interview strategies (reported in both studies) and the second is the correlation found between pre- and post-interview attitudes (documented in Study III). In other words, threateners approached the interview with a set attitude and prepared accordingly. Basic psychological research on persuasion has shown that persons who approach a task

deliberately are less affected by how a particular message is presented (Petty & Cacioppo, 1986).

If threateners are indeed steadfast interviewees, then stronger means are needed to steer their behaviours. In fairness, however, it is still too early to arrive at any definite conclusions. These findings stem from just two laboratory studies and cannot compete with the much stronger body of research on the effectiveness of rapport-based and strategic interviewing (Meissner et al., 2017). Furthermore, it is important to acknowledge that threateners in the current studies may have been unaffected by the *style* of interviewing but not by the *interview* as such. Specifically, the interview impacted the threateners' attitudes and information provision, but this impact was independent of the interview style.

Empirically-Driven Professionals

Study IV examined how professional experience affects the assessment of threats of violence. The results demonstrated that, on average, professionals and non-professionals made almost identical risk assessments, but professionals agreed more with one another. Furthermore, professionals' additional information requests covered more, and more relevant (empirically-based) content as compared to the requests of non-professionals.

The finding of identical risk assessment points towards the notion that the judging of threat cues may in part reflect common sense. Critically, common sense does not necessarily mean bad sense. The assessments of the professionals were found to conform to the literature (i.e. known risk factors were identified as risk increasing and known protective factors were identified as risk decreasing), but so were the assessments of the non-professionals. This result may be explained by literature on risk perception stating that risk assessment is largely affective in nature even when approached rationally, a phenomenon referred to as affective rationality (Damasio, 2001; Slovic & Weber, 2002). It has been theorised that people tend to rely on two different systems when assessing risk in financial, health, and safety domains: an affective system and a cognitive system (Slovic, Finucane, Peters, & MacGregor, 2004). The affective system contains emotional reactions to risk and is inherently present in both experts and novices as responding to threats is deeply rooted in human evolution, while the cognitive system contains, among others, knowledge on probabilities of danger to occur and is more developed in experts than novices (Weber, 2001). This difference is mostly due to experts having a better notion of probabilities, whereas the general public tends to overweight infrequent but catastrophic events (e.g. getting caught up in a terrorist attack; Weber, 2001). However, this typical difference between experts and novices might not always impact risk assessments. The

two systems usually combine to identical risk assessments (Slovic & Weber, 2002), but, when emotional reactions to risk differ from cognitive assessments of risk, emotions are assumed to drive behaviour (Loewenstein, Weber, Hsee, & Welch, 2001). This theory might explain how common sense notions on risk can overrule professional experience when assessing threats of violence. However, the role of emotion in professional threat assessment needs yet to be investigated.

Two other findings suggest that the professionals' performance was superior to that of the non-professionals. These were, higher levels of inter-rater agreement and empirically-driven information searches. Both measures reflect quality standards in expert performance (Dror, 2016; Einhorn, 1974). Agreement between professionals cannot be taken for granted in fields of expertise. To illustrate, studies among forensic experts revealed that their conclusions about DNA evidence, fingerprints, and footwear identifications were often inconsistent (Dror & Hampikian, 2011; Majamaa & Ytti, 1996; Ulery, Hicklin, Buscaglia, & Roberts, 2012). However, it should be noted that these studies examined dichotomous judgements (e.g. Could the suspect have contributed to the DNA mixture?). Such judgements result in clearer inconsistencies as compared to the continuous judgements examined in the current study (e.g. To what extent does this information contribute to the risk for violence?) where the spread in the ratings was used as a proxy for agreement.

The finding that professionals requested empirically-based information more often than non-professionals may reflect a superior ability to make decisions based on relevant information without being biased by irrelevant contextual information (Dror, 2016). Theory and research into expertise suggest that experienced performers (whether criminal investigators, physicians, or other professionals) possess an exceptional understanding of which information is critical to the problem at hand and are quick to recognise this information in a larger bulk of information (Alison, Barrett, & Crego, 2007; Elstein & Schwarz, 2002). These competences help experienced performers generate more and qualitatively better hypotheses as compared to less advanced performers or novices (Fahsing & Ask, 2016; Wright, 2013). Thus, both the current findings and previous research demonstrate that experts know best what information to pursue.

What do these findings mean in practice? First, agreement among professionals is reassuring as it suggests that professionals tend to reach similar conclusions. Second, threat assessment professionals may contribute most to the process of information gathering (as opposed to information assessment). This means that, in a case with limited resources, expertise is best utilised in tasks concerning the information search. For instance, this would involve evaluating what intelligence is missing or setting the scope of a TAM interview.

Limitations

The studies rest on the assumption that social cognitions of people who threaten to cause harm are similar to those of people who do not (i.e. the general public). Hence, it was argued that experimental findings can be generalised as long as basic human dynamics are studied. A limitation of the studies in the thesis is that this assumption was theorised but not tested. Furthermore, the assumption is debatable. Threatening typically involves strong emotions, and personal interests are at stake. Moreover, the type of threats within the field of threat assessment are typically violent threats meaning that the threatener is perpetrating a criminal act by merely uttering the threat. These conditions were not fully mirrored in the design of the studies. Although the current paradigm involved a threat to damage the reputation of the conflicting party, the threat was not inherently illegal or even immoral. Finally, known risk factors in the field of threat assessment (e.g. substance abuse, violent attitudes, and mental illness) were probably underrepresented in the studied samples. Despite the measures taken to maximise external validity (see *Introducing an Experimental Paradigm*) and the notion that real-world resemblance is not always required to examine a phenomenon (Mook, 1983), no direct evidence was obtained on the generalisability of the present findings as the findings stem exclusively from lab-studies of student samples. The question therefore remains whether or not real-world threateners would respond similarly as compared to the participants in the studies.

A number of limitations pertain to the interview protocols employed in the studies. First, the interviews might have come across as rigid to the interviewees. The prompts and questions comprising the protocols were carefully designed, both in phrasing and sequence, and the interviewers were instructed to stick to the protocols. This instruction was given for the sake of experimental control but might have hindered the natural flow of the interactions. Second, the interviews were short, particularly in Studies I and II. It is therefore unlikely they covered all dynamics of TAM interviewing. Third, the manipulations of suspicion (Study II) and rapport (Study III) might have been insufficient to result in the predicted effects. Although manipulation checks were found to be significant, the protocols that were supposed to communicate suspicion and rapport received only moderate ratings in these regards (5.44 and 4.05 on a 7-point Likert scale, respectively).

The studies did not examine a sample from the population of persons who pose a threat without making a threat. These are persons who fully intend to carry out an attack while aiming to remain under the radar, such as many of the suicide bombers attacking in the name of IS.

This group is comparably large and obviously dangerous and, hence, forms a substantial part of the threat assessment domain (Vossekuil et al., 2015). Different interview dynamics could be expected as compared to what was found in the present research. As persons in this group do not seek interaction, they might be less forthcoming and would probably deny having harmful intentions (instead of stressing them when threatening). Thus, the data from the present studies might not apply to these subjects of concern.

Another limitation is that the studies did not test for individual or cultural differences among threateners. Diversity issues are plausibly influential in TAM interviews. Modern societies are increasingly multicultural and threat assessment professionals will likely encounter persons with diverse ethnicities, religions, languages, and cultural practices. Research has shown that interviewees from different cultures can respond differently to interrogation and negotiation tactics such as rational persuasion, authority, and relationship-building (Beune, Giebels, & Sanders, 2009; Beune, Giebels, & Taylor, 2010; Giebels & Taylor, 2012). In a recent publication, Hart (2016b) cast doubt on the cross-cultural validity of risk and threat assessment instruments and appealed to professionals to enhance general awareness of diversity issues. The present research fails to answer this call. Nonetheless, it is acknowledged here that it is important to address cultural and individual differences in research and practice in TAM interviewing (see Future Research).

This final remark is more a nuance than limitation. This thesis does not advocate TAM interviewing as the solution to all threat cases. There are plenty of imaginable circumstances in which authorities should decide to not interview. For instance, cases in which the safety of the interviewer cannot be guaranteed, in which an interview would interfere with an ongoing investigation (and the threat is not imminent), in which the mental condition of the threatener hinders a coherent conversation (e.g. they suffer from a psychosis), or in which it is impossible to reach or trace the threatener (e.g. threatener is located in a warzone; threat is a cyber-threat). However, it is argued here that refraining from interviewing in threat cases should be a conscious decision and not a default scenario.

Future Research

One way of moving TAM interviewing research forward is to increase its sheer quantity. The number of studies examining TAM interviewing is far behind the corpus of interview studies within the related fields of interrogation, negotiation, and intelligence gathering. On a

general level, additional research could refine existing theories and terminology in threat assessment. For instance, is there a difference between risk assessment and threat assessment (discussed on p. 10)? What exactly does targeted violence mean (see p. 1)? How do subjects of concern progress along the pathway towards violence (see p. 6)? There is a need to clarify such conventional yet controversial concepts in the field. More specifically, with regard to TAM interviewing, future research should strengthen and expand the interview manipulation techniques tested in the present studies in order to reach a fuller understanding of interview dynamics in TAM contexts. Furthermore, refinements to the current set-up should be made to optimise the balance between the reality of a threat paradigm, the real-life relevance of the paradigm to the participant sample, and research ethics. The realism of the paradigm might be improved by having participants threaten with an illegal act, for instance, to leak information covered by a confidentiality agreement signed by participants. Replications could further contribute to the robustness of the current findings, especially if conducted across different labs and samples. Eventually, mechanisms examined in laboratory studies must be tested in applied settings to prove the assumption of generalisability (see Limitations).

The generalisability of interview approaches is limited by individual and cultural differences. There is a need to explore these limitations so that interview approaches can be customised for specific target groups. It has been suggested that cultural norms and values become more prominent under stress, meaning that stress leads people to fall back on the cultural habits with which they were raised, such as their native language (Giebels & Taylor, 2012). Yet, cultural issues are not sufficiently studied within the field of threat assessment (Hart, 2016b). Cultural frameworks that could be explored include the distinction between low-context cultures (i.e. cultures that use more direct and content-oriented communication) and high-context cultures (i.e. cultures that use more indirect and context-oriented communication; Giebels & Taylor, 2012) and, in the light of terrorism, aspects of Western and Muslim subcultures. Moreover, some individual characteristics are worth studying. For instance, researchers examining real-world interviews with extremists and terrorists have noted that such interviewees display little self-reflection (Alison, 2016) and strong dualistic worldviews (e.g. us/them, good/bad; Dalgaard-Nielsen, 2013). Future studies should incorporate measures that tap into these individual/group belief systems. Such research may help to establish a good fit between interview objective, interview strategy, and interviewee.

A topic that might broaden the scope of future research is interviewing as a *means* to managing a threatening situation. The typical aim of TAM interviewing is to gather information to assess risk and recommend intervention measures. However, interviewing could also be

employed to steer the threatener away from violence. One strategy to evoke change in others is motivational interviewing (Miller, 1983). Motivational interviewing is typically used in clinical settings and rests on the idea that people are best persuaded by arguments they hear themselves defend. In other words, it is assumed that clients are more inclined to change destructive behaviours if they can bring up their own motives for change, instead of listening to arguments presented by others. Hence, the therapist tries to encourage the patient to talk about motivations for change, so-called “change talk”. Numerous studies have proven the efficacy of motivational interviewing (Hettema, Steele, & Miller, 2005). Another threat management strategy could be the use of counter-narratives (Dalgaard-Nielsen, 2013). Counter-narratives are stories providing a view of the world that challenges the narratives supporting violence or extremism (Braddock & Horgan, 2016). Counter-narratives are intended to cast doubt on a threatener’s plan or ideology in order to alter dangerous worldviews. While the use of counter-narratives is considered one of the U.S.’s core strategies in preventing extremist ideologies, researchers have only recently turned their attention to the development of evidence-based narratives (Beutel, et al., 2016; Braddock & Horgan, 2016). Finally, threat managers may use an interview to reach out to a threatener to offer practical help (James et al., 2010) or to seek mutual gain (Shapiro, 2006). None of these strategies have been systematically tested in a TAM context. Yet, each of them may benefit threat management outcomes such as increased cooperation, higher likelihood of future interactions being constructive, de-escalation, and, ultimately, refrainment from violence.

Currently, little is known about how or how well professionals interview threateners. The study of professionals included in this thesis (Study IV) examines what information they would search for when making a threat assessment. However, to address professionals’ skills for TAM interviewing, future research should include measures on how they would conduct an interview with a person of concern. For instance, to list the questions and explain the strategies that they would ask in a given case. Such direct measures, in which they actually perform a threat management task, might give more insight into their competence than questionnaires in which they are supposed to reflect on their daily work (e.g. “How do you typically perform this task”; “How do you think this task should be performed?”).

Ethical Considerations

TAM interviewing in the laboratory

The experimental paradigm used in Studies I, II, and III required participants to make a threat or to discuss a threat they had made. The act of threatening as well as discussing the threat might have been stressful for the participants. Several efforts were made to minimise a potentially negative experience for the participants. To avoid or reduce moral constraints, the case given to participants was phrased in such a way that participants represented the party that was right according to widely accepted moral values and were to threaten a party that was morally wrong. Also, the harm participants threatened to inflict was not violent or otherwise unlawful but instead implied financial/reputational damage.

To further ensure ethical research practices, all participants read and signed an informed consent in which they agreed to have understood participation is voluntary, confidential, and that the data would only be used for research purposes. The document specifically stated they were allowed to quit at any point in time. This, in fact, was done by 21 out of 496 participants (4.2%) because they felt uncomfortable with the interactive part of the study. They received full compensation. In the debriefing, all participants were given the opportunity to share their thoughts on the experiment. Subsequently, they were informed of the actual goal of the research, the position of the interviewer, the fictitious nature of the case, and, furthermore, it was emphasised that no one acted correctly or incorrectly in the experiment as there was no correct or incorrect behaviour.

Approval for the studies was obtained from the Regional Ethical Review Board in Gothenburg (Studies I, II, and III) and the ethics committee at the University of Portsmouth (Study IV). For favourable decisions received, see Appendix A.

TAM interviewing in practice

Practitioners in the field of threat assessment and management can have many different professional backgrounds (e.g. police, law, medicine, behavioural science, security). Some professionals operate under governmental flags while others work for corporate businesses or run private consulting firms. Moreover, some professionals are full-time threat managers while others perform TAM tasks as an integral part of their jobs. The large diversity among threat assessment and management professionals is challenging to ethical conduct, but several efforts toward professionalisation have been made over the past three decades. For instance, the

American Threat Assessment Association published a code of conduct outlining professional standards of ethical practices (ATAP Code of Ethical Conduct, 2010). In addition, training and certification programmes have been developed and, since 2015, practitioners can apply for a “Threat Manager Certificate” that is awarded by ATAP.

Despite these efforts, steps are yet to be taken to guarantee qualitative, ethical, and lawful practices in threat assessment and management. One of these steps is the further expansion of professionalisation from the US to other parts of the world. This trend is emerging with the rise of Canadian, European, and Asian sister organisations of ATAP. However, these organisations are much smaller than ATAP and, although accreditation processes are in progress, they are still in their infancies.

Another step forward would be to develop conduct codes into more concrete implications for TAM interviewing (and other TAM tasks). For instance, it is stated in the conduct code that professionals should operate within the boundaries of their competence, and that they should respect privacy and confidentiality—but what does this mean in practice? Who exactly is authorised to conduct TAM interviews? Under what circumstances should these interviews take place? Can the interviewee refuse to take part? Who is responsible for managing the aftermath of the interview, including possible escalation? These questions remain unanswered.

Finally, there exists no legal authority to guard ethical or lawful conduct in the field of threat assessment and management. Certified expertise thus stands or falls with acknowledgement in the field. Acknowledgement here means that professionals, clients, and organisations are aware of quality standards and choose to live up to these. Developing such a support base takes time and effort. However, as long as certification is not required by law, TAM practitioners remain free to practice their work however they see fit as long as it does not conflict with criminal law, civil law, or laws applying to their particular profession.

Conclusions

Current threat assessment and management (TAM) interviewing draws on customary knowledge, which can be explained as knowledge that has emerged over time and through experience and has been passed on through observational learning and storytelling (Hartwig et al., 2014). The present thesis seeks to advance this knowledge by proposing a science-based perspective on effective TAM interviewing; what dynamics can be expected and, given these

dynamics, what interview methods work best? Combining the theory and findings presented in this thesis, it could be concluded that threateners are semi-cooperative interviewees whose attitudes and behaviours may not be significantly influenced by general interview approaches (e.g. rapport-based interviewing, suspicion-oriented interviewing). Instead, the findings point to a need for more strategic approaches that (i) are developed from the perspective of the threatener so his/her existing attitudes can be anticipated and exploited, (ii) make the threatener's motivation to be informative prevail over the need to be strategic, and (iii) strike a balance between controlling risk (by making risk assessments and placing restrictions) and meeting needs (by reaching out to the threatener and working towards a solution). Science-based interview techniques should be developed that tap into one or more of these preliminary findings. Such developments will most likely improve the quality of TAM interviewing but may also lower the threshold for conducting such an interview in the first place. In turn, more real-world interviewing will give rise to new experiences and data that can serve as input for future research. It is this interplay between science and practice that is needed to advance the field of threat assessment and management.

REFERENCES

- Alison, L. (2016, June). *Why tough tactics fail and rapport gets results: A focus on accessing deep held beliefs*. Presented at the 9th annual conference of the International Investigative Interviewing Research Group (IIIRG) & Masterclass, Chesham, UK.
- Alison, L. J., Alison, E., Noone, G., Elntib, S., & Christiansen, P. (2013). Why tough tactics fail and rapport gets results: Observing Rapport-Based Interpersonal Techniques (ORBIT) to generate useful information from terrorists. *Psychology, Public Policy, and Law*, 19, 411-431. doi: 10.1037/a0034564
- Alison, L., Alison, E., Noone, G., Elntib, S., Waring, S., & Christiansen, P. (2014a). Whatever you say, say nothing: Individual differences in counter interrogation tactics amongst a field sample of right wing, AQ inspired and paramilitary terrorists. *Personality and Individual Differences*, 68, 170-175. doi.org/10.1016/j.paid.2014.04.031
- Alison, L., Alison, E., Noone, G., Elntib, S., Waring, S., & Christiansen, P. (2014b). The efficacy of rapport-based techniques for minimizing counter-interrogation tactics amongst a field sample of terrorists. *Psychology, Public Policy, and Law*, 20, 421-430. doi.org/10.1037/law0000021
- Alison, L., Barrett, E., & Crego, J. (2007). Criminal investigative decision making: Context and process. In R. R., Hoffman (Ed.), *Expertise out of context: Proceedings of the sixth international conference on naturalistic decision making* (pp. 79-95). London & New York: Taylor & Francis Group.
- Ask, K., Granhag, P. A., Juhlin, F., & Vrij, A. (2013). Intending or pretending? Automatic evaluations of goal cues discriminate true and false intentions. *Applied Cognitive Psychology*, 27, 173-177. doi.org/10.1002/acp.2893
- ATAP Code of Ethical Conduct (2010). Retrieved from <http://c.ymcdn.com/sites/www.atapworldwide.org/resource/resmgr/imported/documents/ATAP-code-of-ethics.pdf>
- Beune, K., Giebels, E., & Sanders, K. (2009). Are you talking to me? Influencing behaviour and culture in police interviews. *Psychology, Crime & Law*, 15, 597-617. doi.org/10.1080/10683160802442835
- Beune, K., Giebels, E., & Taylor, P. J. (2010). Patterns of interaction in police interviews: The role of cultural dependency. *Criminal Justice and Behavior*, 37, 904-925. doi.org/10.1177/0093854810369623
- Beutel, A., Weine, S., Saeed, A., Mihajlovic, A., Stone, A., Beahrs, J., & Shanfield, S. (2016).

- Guiding Principles for Countering and Displacing Extremist Narratives. *Journal of Terrorism Research*, 7, 35-49. doi.org/10.15664/jtr.1220
- Boer, D.P., Hart, S.D., Kropp, P.R., & Webster, C.D. (1997). *Manual for the Sexual Violence Risk –20: Professional guidelines for assessing risk of sexual violence*. Vancouver, B.C.: The Mental Health, Law, and Policy Institute.
- Bogaard, G., Meijer, E. H., Vrij, A., & Merckelbach, H. (2016). Strong, but wrong: lay people's and police officers' beliefs about verbal and nonverbal cues to deception. *PloS ONE*, 11. doi.org/10.1371/journal.pone.0156615
- Bond, C. F., & DePaulo, B. M. (2006). Accuracy of deception judgments. *Personality and Social Psychology Review*, 10, 214-234. doi: 10.1207/s15327957pspr1003_2
- Borum, R., Fein, R., Vossekuil, B., & Berglund, J. (1999). Threat assessment: Defining an approach to assessing risk for targeted violence. *Behavioral Sciences & the Law*, 17, 323-337. doi.org/10.1002/(SICI)10990798(199907/09)17:3<323::AIDBSL349>3.0.CO;2-G
- Braddock, K., & Horgan, J. (2016). Towards a Guide for Constructing and Disseminating Counternarratives to Reduce Support for Terrorism. *Studies in Conflict and Terrorism*, 39, 381-404. doi.org.ezproxy.ub.gu.se/10.1080/1057610X.2015.1116277
- Brandon, S. E. (2011). Impacts of psychological science on national security agencies post-9/11. *American Psychologist*, 66, 495-506. doi.org/10.1037/a0024818
- Bull, R. (2013). What is 'believed' or actually 'known' about characteristics that may contribute to being a good/effective interviewer. *Investigative Interviewing: Research and Practice*, 5, 128-143.
- Calhoun, F. S., & Weston, S. W. (2003). *Contemporary threat management: A practical guide for identifying, assessing, and managing individuals of violent intent*. San Diego, CA: Specialised Training Services.
- Calhoun, F. S., & Weston, S. W. (2015). Perspectives on threat management. *Journal of Threat Assessment and Management*, 2, 258-267. doi.org/10.1037/tam0000056
- Campbell, M. A., French, S., & Gendreau, P. (2009). The prediction of violence in adult offenders a meta-analytic comparison of instruments and methods of assessment. *Criminal Justice and Behavior*, 36, 567-590. doi.org/10.1177/0093854809333610
- Corner, E., & Gill, P. (2015). A false dichotomy? Mental illness and lone-actor terrorism. *Law and Human Behavior*, 39, 23-34. doi.org/10.1037/lhb0000102
- Dalgaard-Nielsen, A. (2013). Promoting exit from violent extremism: Themes and approaches. *Studies in Conflict & Terrorism*, 36, 99-115. doi.org/10.1080/1057610X.2013.747073

- Damasio, A. R. (2001). Emotion and the human brain. *Annals of the New York Academy of Sciences*, 935, 101-106. doi.org/10.1111/j.1749-6632.2001.tb03475.x
- DePaulo, B. M. (1992). Nonverbal behavior and self-presentation. *Psychological Bulletin*, 111, 203-243. doi.org/10.1037/0033-2909.111.2.203
- Dietz, P. E., Matthews, D. B., Van Duyne, C., Martell, D. A., Parry, C. D., Stewart, T., ... & Crowder, J. D. (1991). Threatening and otherwise inappropriate letters to Hollywood celebrities. *Journal of Forensic Science*, 36, 185-209. doi.org/10.1520/jfs13019j
- Douglas, K. S., Hart, S. D., Webster, C. D., Belfrage, H., Guy, L. S., & Wilson, C. M. (2014). Historical-clinical-risk management-20, version 3 (HCR-20V3): development and overview. *International Journal of Forensic Mental Health*, 13, 93-108. doi.org/10.1080/14999013.2014.906519
- Dror, I. E. (2016). A hierarchy of Expert Performance. *Journal of Applied Research in Memory and Cognition*, 5, 121-127. doi.org/10.1016/j.jarmac.2016.03.001
- Dror, I. E., & Hampikian, G. (2011). Subjectivity and bias in forensic DNA mixture interpretation. *Science & Justice*, 51, 204-208. doi.org/10.1016/j.scijus.2011.08.004
- Einhorn, H. J. (1974). Expert judgment: Some necessary conditions and an example. *Journal of Applied Psychology*, 59, 562-571. doi.org/10.1037/h0037164
- Elliot, A. J. (Ed.). (2008). *Handbook of approach and avoidance motivation*. New York: Psychology Press.
- Elstein, A. S., & Schwarz, A. (2002). Clinical problem solving and diagnostic decision making: Selective review of the cognitive literature. *British Medical Journal*, 324, 729-732. doi.org/10.1136/bmj.324.7339.729
- Evans, J. R., Houston, K. A., Meissner, C. A., Ross, A. B., LaBianca, J. R., Woestehoff, S. A., & Kleinman, S. M. (2014). An empirical evaluation of intelligence-gathering interrogation techniques from the United States Army field manual. *Applied Cognitive Psychology*, 28, 867-875. https://doi.org/10.1002/acp.3065
- Evans, J. R., Meissner, C. A., Brandon, S. E., Russano, M. B., & Kleinman, S. M. (2010). Criminal versus HUMINT interrogations: The importance of psychological science to improving interrogative practice. *The Journal of Psychiatry & Law*, 38, 215-249. doi.org/10.1177/009318531003800110
- Fahsing, I., & Ask, K. (2016). The making of an expert detective: the role of experience in English and Norwegian police officers' investigative decision-making. *Psychology, Crime & Law*, 22, 203-223. doi.org/10.1080/1068316X.2015.1077249

- Fein, R. A., & Vossekuil, B. (1998). *Protective intelligence and threat assessment investigations: A guide for state and local law enforcement officials*. Washington, DC: US Department of Justice, Office of Justice Programs, National Institute of Justice.
- Fein, R. A., & Vossekuil, B. (1999). Assassination in the United States: An operational study of recent assassins, attackers, and near-lethal approachers. *Journal of Forensic Science*, 44, 321-333. doi.org/10.1520/JFS14457J
- Fein, R. A., Vossekuil, B., & Holden, G. A. (1995). *Threat assessment: An approach to prevent targeted violence*, 2. Washington, DC: US Department of Justice, Office of Justice Programs, National Institute of Justice.
- Ferguson, M. J., & Bargh, J. A. (2004). Liking is for doing: the effects of goal pursuit on automatic evaluation. *Journal of Personality and Social Psychology*, 87, 557-572. doi.org/10.1037/0022-3514.87.5.557
- Fiske, S. T., & Macrae, C. N. (Eds.). (2012). *The SAGE handbook of social cognition*. London, UK: SAGE Publications Ltd.
- Galinsky, A. D., Maddux, W. W., Gilin, D., & White, J. B. (2008). Why it pays to get inside the head of your opponent: The differential effects of perspective taking and empathy in negotiations. *Psychological Science*, 19, 378-384. doi.org/10.1111/j.1467-9280.2008.02096.x
- Giebels, E., & Taylor, P. J. (2010). Communication predictors and social influence in crisis negotiations. In R. G. Rogan & F. J. Lanceley (Eds.), *Contemporary theory, research, and practice of crisis/hostage negotiations*. New York, NY: Hampton Press.
- Giebels, E., & Taylor, P. J. (2012). Tuning in to the right wavelength: The importance of culture for effective crisis negotiation. In M. St-Yves & P. L. Collins (Eds.), *The psychology of crisis intervention for law enforcement officers* (pp. 277-294). Montreal, Canada: Éditions Yvon Blais.
- Gill, P. (2015). Toward a scientific approach to identifying and understanding indicators of radicalization and terrorist intent: Eight key problems. *Journal of Threat Assessment and Management*, 2, 187-191. doi.org/10.1037/tam0000047
- Gill, P., Horgan, J., Corner, E., & Silver, J. (2016). Indicators of lone actor violent events: The problems of low base rates and long observational periods. *Journal of Threat Assessment and Management*, 3, 165-173. doi.org/10.1037/tam0000066
- Gollwitzer, P. M. (1999). Implementation intentions: Strong effects of simple plans. *American Psychologist*, 54, 493-503. doi.org/10.1037/0003-066X.54.7.493

- Gollwitzer, P. M., & Sheeran, P. (2006). Implementation intentions and goal achievement: A meta-analysis of effects and processes. *Advances in Experimental Social Psychology*, 38, 69-119. doi.org/10.1016/S0065-2601(06)38002-1
- Granhag, P. A. (2010). On the psycho-legal study of true and false intentions: Dangerous waters and some stepping stones. *The Open Criminology Journal*, 3, 37-43. doi.org/10.2174/1874917801003020037
- Granhag, P. A., & Hartwig, M. (2008). A new theoretical perspective on deception detection: On the psychology of instrumental mind-reading. *Psychology, Crime & Law*, 14, 189-200. doi: 10.1080/10683160701645181
- Granhag, P. A., & Hartwig, M. (2015). The strategic use of evidence technique: A conceptual overview. In P. A. Granhag, A. Vrij, & B. Verschuere (Eds.), *Detecting deception: Current challenges and cognitive approaches* (pp. 231-251), Chichester, UK: Wiley Blackwell.
- Granhag, P. A., Hartwig, M., Mac Giolla, E. M., & Clemens, F. (2015). Suspects' verbal counter-interrogation strategies. In P. A. Granhag, A. Vrij, & B. Verschuere (Eds.), *Detecting deception: Current challenges and cognitive approaches* (pp. 293-313), Chichester, UK: Wiley Blackwell.
- Granhag, P. A., Kleinman, S. M., & Oleszkiewicz, S. (2016). The Scharff technique: On how to effectively elicit intelligence from human sources. *International Journal of Intelligence and Counter-Intelligence*, 29, 132-150. doi.org/10.1080/08850607.2015.1083341
- Granhag, P. A., & Knieps, M. (2011). Episodic future thought: Illuminating the trademarks of forming true and false intentions. *Applied Cognitive Psychology*, 25, 274-280. doi.org/10.1002/acp.1674
- Granhag, P. A., & Mac Giolla, E. (2014). Preventing future crimes. *European Psychologist*, 19, 195-206. doi.org/10.1027/1016-9040/a000202
- Guy, L. S. (2008). *Performance indicators of the structured professional judgment approach for assessing risk for violence to others: A meta-analytic survey* (Doctoral dissertation). Retrieved from Simon Fraser University: http://s3.amazonaws.com/academia.edu.documents/24186984/etd4194.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1497283814&Signature=mmjaaPCSzeHxvmlxEAzxnmqwZcI%3D&response-content-disposition=inline%3B%20filename%3DPerformance_indicators_of_the_structured.pdf.
- Guy, L. S., (Guest Ed.) (2015). ATAP's 25th annual threat management conference. [Special

- Section]. *Journal of Threat Assessment and Management*, 2, 227-274.
- Guy, L. S., Packer, I. K., & Warnken, W. (2012). Assessing risk for violence using structured professional judgment guidelines. *Journal of Forensic Psychology Practice*, 12, 270-283. doi.org/10.1080/15228932.2012.674471
- Hall, R. C., Platt, D. E., & Hall, R. C. (1999). Suicide risk assessment: a review of risk factors for suicide in 100 patients who made severe suicide attempts: evaluation of suicide risk in a time of managed care. *Psychosomatics*, 40, 18-27. https://doi.org/10.1016/S0033-3182(99)71267-3
- Harris, G. T., Rice, M. E., & Quinsey, V. L. (1993). Violent recidivism of mentally disordered offenders: The development of a statistical prediction instrument. *Criminal Justice and Behavior*, 20, 315–335. doi:10.1177/0093854893020004001
- Hart, S. D. (2016a, April). *Some thorny issues in threat assessment*. Paper presented at the AETAP Annual Meeting, Ghent, Belgium.
- Hart, S. D. (2016b). Culture and violence risk assessment: The case of Ewert v. Canada. *Journal of Threat Assessment and Management*, 3, 76-96. doi.org/10.1037/tam0000068
- Hart, S. D., Hoffmann, J., de Vogel, V., & Kropp, R. (2015, April). *Expert panel Threat vs. risk assessment*. Panel discussion conducted at the 8th conference of the Association of European Threat Assessment Professionals, Lucerne, Switzerland.
- Hartwig, M., Granhag, P. A., & Luke, T. (2014). Strategic use of evidence during investigative interviews: The state of the science. In D. C., Raskin, C. R. Honts, & J. C. Kircher (Eds), *Credibility assessment: Scientific research and applications* (pp. 1- 36). doi.org/10.1016/B978-0-12-394433-7.00001-4
- Hartwig, M., Granhag, P. A., & Strömwall, L. A. (2007). Guilty and innocent suspects' strategies during police interrogations. *Psychology, Crime & Law*, 13, 213-227. doi: 10.1080/10683160600750264
- Hartwig, M., Granhag, P. A., Strömwall, L. A., & Doering, N. (2010). Impression and Information management: On the strategic self-regulation of innocent and guilty suspects. *The Open Criminology Journal*, 3, 10-16. doi.org/10.2174/1874917801003010010
- Hartwig, M., Luke, T. J., & Skerker, M. (2016). Ethical perspectives on interrogation. In J. Jacobs & J. Jackson (Eds.), *The Routledge handbook of criminal justice ethics* (pp. 326-347). London and New York: Taylor & Francis Group.
- Hartwig, M., Meissner, C. A., & Semel, M. D. (2014). Human intelligence interviewing and

- interrogation: Assessing the challenges of developing an ethical, evidence-based approach. In R. Bull (Ed.), *Investigative interviewing* (pp. 209-228). New York: Springer. doi: 10.1007/978-1-4614-9642-7_11
- Heilbrun, K., Yasuhara, K., & Shah, S. (2010). Violence risk assessment tools. In R. K. Otto, & K. S. Douglas (Eds.), *Handbook of violence risk assessment* (1-18). London and New York: Taylor & Francis Group.
- Hettema, J., Steele, J., & Miller, W. R. (2005). Motivational interviewing. *Annual Review of Clinical Psychology*, 1, 91-111. doi: 10.1146/annurev.clinpsy.1.102803.143833
- Hines, A., Colwell, K., Hiscock-Anisman, C., Garrett, E., Ansarra, R., & Montalvo, L. (2010). Impression management strategies of deceivers and honest reporters in an investigative interview. *The European Journal of Psychology Applied to Legal Context*, 2, 73-90.
- Hoffmann, J. (2009). Public figures and stalking in the European context. *European Journal on Criminal Policy and Research*, 15, 293-305. <https://doi.org/10.1007/s10610-009-9104-0>
- Home Office (2003). *Police and criminal evidence act 1984. Codes of practice A-E revised edition*. London: HMSO. Retrieved from: www.legislation.gov.uk/ukpga/1984/60/pdfs/ukpga_19840060_en.pdf
- Inbau, F. E., Reid, J. E., Buckley, J. P., & Jayne, B. C. (2011). *Criminal interrogation and Confessions*. Massachusetts, USA: Jones & Bartlett Publishers.
- James, D. V., & Farnham, F. R. (2016). Outcome and efficacy of interventions by a public figure threat assessment and management unit: a mirrored study of concerning behaviors and police contacts before and after intervention. *Behavioral Sciences & the Law*, 34, 660-680. doi.org/10.1002/bsl.2255
- James, D. V., Kerrigan, T. R., Forfar, R., Farnham, F. R., & Preston, L. F. (2010). The Fixated Threat Assessment Centre: preventing harm and facilitating care. *The Journal of Forensic Psychiatry & Psychology*, 21, 521-536. doi.org/10.1080/14789941003596981
- James, D. V., MacKenzie, R. D., & Farnham, F. R. (2014). *Communications Threat Assessment Protocol*. London: Theseus LLP.
- James, D. V., Mullen, P. E., Pathé, M. T., Meloy, J. R., Preston, L. F., Darnley, B., & Farnham, F. R. (2009). Stalkers and harassers of royalty: the role of mental illness and motivation. *Psychological Medicine*, 39, 1479-1490. doi.org/10.1017/S0033291709005443
- Jonckheere, A. R. (1954). A distribution-free k-sample test against ordered alternatives. *Biometrika*, 41, 133-145. doi: 10.2307/2333011.

- Justice, B. P., Bhatt, S., Brandon, S. E., & Kleinman, S. M. (2010). *Army field manual 2-22.3 interrogation methods: A science-based review*. Washington, DC (Draft, September).
- Kebbell, M., Hurren, E., & Mazerolle, P. (2006). *An investigation into the effective and ethical interviewing of suspected sex offenders*. Retrieved from Australian Institute of Criminology: <http://crg.aic.gov.au/reports/200304-12.pdf>
- Kelleher, M. D. (1997). *Profiling the lethal employee: Case studies of violence in the workplace*. Connecticut, USA: Greenwood Publishing Group.
- Knieps, M., Granhag, P. A., & Vrij, A. (2013). Back to the future: Asking about mental images to discriminate between true and false intentions. *The Journal of Psychology*, 147, 619-640. doi.org/10.1080/00223980.2012.728542
- Leo, R. A. (1996). Inside the interrogation room. *The Journal of Criminal Law and Criminology*, 86, 266-303. doi.org/10.2307/1144028
- Liberman, N., & Trope, Y. (1998). The role of feasibility and desirability considerations in near and distant future decisions: A test of temporal construal theory. *Journal of Personality and Social Psychology*, 75, 5-18. doi: 10.1037/0022-3514.75.1.5
- Loewenstein, G. F., Weber, E. U., Hsee, C. K., & Welch, N. (2001). Risk as feelings. *Psychological Bulletin*, 127, 267-286. doi.org/10.1037/0033-2909.127.2.267
- Luke, T. J., Dawson, E., Hartwig, M., & Granhag, P. A. (2014). How awareness of possible evidence induces forthcoming counter-interrogation strategies. *Applied Cognitive Psychology*, 28, 876-882. doi.org/10.1002/acp.3019
- Mac Giolla, E., & Granhag, P. A. (2015). Detecting false intent amongst small cells of suspects: single versus repeated interviews. *Journal of Investigative Psychology and Offender Profiling*, 12, 142-157. doi.org/10.1002/jip.1419
- Mac Giolla, E., Granhag, P. A., & Liu-Jönsson, M. (2013). Markers of good planning behavior as a cue for separating true and false intent. *PsyCh Journal*, 2, 183-189. doi:10.1002/pchj.36
- MacKenzie, R. D., McEwan, T. E., Pathé, M. T., James, D. V., Ogloff, J. R. P., & Mullen, P. E. (2009). *The Stalking Risk Profile. Guidelines for assessing and managing stalkers*. Melbourne: StalkInc. & Centre for Forensic Behavioural Science, Monash University.
- Majamaa, H., & Ytti, A. (1996). A survey of the conclusions drawn of similar footwear cases in various crime laboratories. *Forensic Science International*, 82, 109-120. doi.org/10.1016/0379-0738(96)01972-X

- Malle, B. F., & Knobe, J. (1997). The folk concept of intentionality. *Journal of Experimental Social Psychology*, 33, 101-121. doi.org/10.1006/jesp.1996.1314
- Meehl, P. E., & Rosen, A. (1955). Antecedent probability and the efficiency of psychometric signs, patterns, or cutting scores. *Psychological Bulletin*, 52, 194-216. doi.org/10.1037/h0048070
- Meissner, C. A., Redlich, A. D., Michael, S. W., Evans, J. R., Camilletti, C. R., Bhatt, S., & Brandon, S. (2014). Accusatorial and information-gathering interrogation methods and their effects on true and false confessions: A meta-analytic review. *Journal of Experimental Criminology*, 10, 459-486. doi.org/10.1007/s11292-014-9207-6
- Meissner, C. A., Surmon-Böhr, F., Oleszkiewicz, S., & Alison, L. (2017). *Developing an evidence-based perspective on what works in the interrogation of suspects: A review of the U.S. government's high-value detainee interrogation group research program*. Manuscript submitted for publication.
- Meloy, J. R. (2015). Threat assessment: Scholars, operators, our past, our future. *Journal of Threat Assessment and Management*, 2, 231-242. doi.org/10.1037/tam0000054
- Meloy, J. R., & Gill, P. (2016). The lone-actor terrorist and the TRAP-18. *Journal of Threat Assessment and Management*, 3, 37-52. doi.org/10.1037/tam0000061
- Meloy, J. R., Hart, S. D., & Hoffmann, J. (2014a). Threat assessment and threat management. In J. R. Meloy & J. Hoffmann (Eds.), *International handbook of threat assessment* (pp. 3-17). New York, NY: Oxford University Press.
- Meloy, R. J., Hoffmann, J., Guldemann, A., & James, D. (2012). The role of warning behaviors in threat assessment: An exploration and suggested typology. *Behavioral Sciences & the Law*, 30, 256-279. doi.org/10.1002/bsl.999
- Meloy, J. R., Hoffmann, J., Roshdi, K., Glaz-Ocik, J., & Guldemann, A. (2014b). Warning behaviors and their configurations across various domains of targeted violence. In J. R. Meloy & J. Hoffmann (Eds.), *International handbook of threat assessment* (pp. 39-53). New York, NY: Oxford University Press.
- Meloy, J. R., James, D. V., Mullen, P. E., Pathé, M. T., Farnham, F. R., Preston, L. F., & Darnley, B. J. (2011). Factors associated with escalation and problematic approaches toward public figures. *Journal of Forensic Sciences*, 56, 128-135. doi.org/10.1111/j.1556-4029.2010.01574.x
- Meloy, J. R., & Mohandie, K. (2014). Assessing threats by direct interview of the violent true believer. In J. R. Meloy & J. Hoffmann (Eds.), *International handbook of threat assessment* (pp. 388-398). New York, NY: Oxford University Press.

- Meloy, J. R., Roshdi, K., Glaz-Ocik, J., & Hoffmann, J. (2015). Investigating the individual terrorist in Europe. *Journal of Threat Assessment and Management*, 2, 140-152. doi.org/10.1037/tam0000036
- Meloy, J. R., White, S. G., & Hart, S. (2013). Workplace assessment of targeted violence risk: The development and reliability of the WAVR-21. *Journal of forensic sciences*, 58, 1353-1358. doi.org/10.1111/1556-4029.12196
- Memon, A., Meissner, C. A., & Fraser, J. (2010). The Cognitive Interview: A meta-analytic review and study space analysis of the past 25 years. *Psychology, Public Policy, and Law*, 16, 340–372. doi:10.1037/a0020518
- Milburn, T. W., & Watman, K. H. (1981). *On the nature of threat: A social psychological analysis*. New York, NY: Praeger Publishers.
- Miller, W. R. (1983). Motivational interviewing with problem drinkers. *Behavioural Psychotherapy*, 11, 147-172. doi.org/10.1017/S0141347300006583
- Milne, B., Shaw, G., & Bull, R. (2007). Investigative interviewing: The role of research. In D. Carson, R. Milne, F. Pakes, K. Shalev, & A. Shawyer (Eds.). *Applying psychology to criminal justice* (pp. 65-80). Chichester: John Wiley & Sons.
- Mohandie, K. (2014). Threat Assessment in Schools. In J. R. Meloy & J. Hoffmann (Eds.), *International handbook of threat assessment* (pp. 126-147). New York, NY: Oxford
- Mook, D. G. (1983). In defense of external invalidity. *American Psychologist*, 38, 379-387. doi.org/10.1037/0003-066X.38.4.379
- Mullen, P. E., James, D. V., Meloy, J. R., Pathé, M. T., Farnham, F. R., Preston, L., ... & Berman, J. (2009). The fixated and the pursuit of public figures. *The Journal of Forensic Psychiatry & Psychology*, 20, 33-47. doi.org/10.1080/14789940802197074
- O'Connor, T., & Carson, W. (2005). Understanding the psychology of child molesters: A key to getting confessions. *Police Chief*, 72, 70-78.
- Oleszkiewicz, S. (2016). *Eliciting human intelligence: A conceptualization and empirical testing of the Scharff technique* (Doctoral dissertation). Retrieved from Gothenburg University: https://gupea.ub.gu.se/bitstream/2077/41567/1/gupea_2077_41567_1.pdf
- Oleszkiewicz, S., Granhag, P. A., & Cancino Montecinos, S. (2014). The Scharff-technique: Eliciting intelligence from human sources. *Law and Human Behavior*, 38, 478. doi.org/10.1037/lhb0000085
- Oleszkiewicz, S., Granhag, P. A., & Kleinman, S. M. (2017). Gathering human intelligence via repeated interviewing: Further empirical tests of the Scharff technique.

- Psychology, Crime & Law*. Advanced online publication.
doi.org/10.1080/1068316x.2017.1296150
- Oostinga, M. S. D., Giebels, E., & Taylor, P. J. (2017). *Walking on thin ice: An experimental exploration of communication error management in law enforcement interactions*. Manuscript submitted for publication.
- O'Toole, M. E. (2009). *The school shooter: A threat assessment perspective*. Quantico, Virginia: National Center for the Analysis of Violent Crime (NCAVC), FBI Academy
- Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. *Advances in Experimental Social Psychology*, 19, 124-205. doi.org/10.1016/S0065-2601(08)60214-2
- Reddy, M., Borum, R., Berglund, J., Vossekuil, B., Fein, R., & Modzeleski, W. (2001). Evaluating risk for targeted violence in schools: Comparing risk assessment, threat assessment, and other approaches. *Psychology in the Schools*, 38, 157-172. doi.org/10.1002/pits.1007
- Rogan, R. G., Hammer, M. R., & van Zandt, C. R. (1994). Profiling crisis negotiation teams. *Police Chief*, 61, 14-14.
- Rosenfeld, B., & Harmon, R. (2002). Factors associated with violence in stalking and obsessional harassment cases. *Criminal Justice and Behavior*, 29, 671-691. doi.org/10.1177/009385402237998
- Saywitz, K. J., Larson, R. P., Hobbs, S. D., & Wells, C. R. (2015). Developing rapport with children in forensic interviews: Systematic review of experimental research. *Behavioral Sciences & the Law*, 33, 372-389. doi: 10.1002/bsl.2186
- Scalora, M. J., Baumgartner, J. V., Zimmerman, W., Callaway, D., Maillette, M. H., Covell, C. N., ... & Washington, D. O. (2002). An epidemiological assessment of problematic contacts to members of Congress. *Journal of Forensic Science*, 47, 1360-1364. doi.org/10.1520/JFS15575J
- Shapiro, D. L. (2006). Negotiation theory and practice: Exploring ideas to aid information education. In Fein, R. A., Lehner, P., & Vossekuil, B. (Eds.) *Educating information-interrogation: Science and art, foundations for the future* (pp. 267-284). Washington, DC: National Defense Intelligence College.
- Sheeran, P., Milne, S., Webb, T. L., & Gollwitzer, P. M. (2005). Implementation intentions and health behavior. In M. Conner & P. Norman (Eds.), *Predicting Health Behavior: Research and Practice with Social Cognition Models* (pp. 276-323). Milton Keynes, UK: Open University Press.

- Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2004). Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk Analysis*, 24, 311-322. doi.org/10.1111/j.0272-4332.2004.00433.x
- Slovic, P., & Weber, E. U. (2002, April). *Perception of risk posed by extreme events*. Paper prepared for discussion at the conference Risk Management Strategies in an Uncertain World, New York.
- Soderberg, C. K., Callahan, S. P., Kochersberger, A. O., Amit, E., & Ledgerwood, A. (2014). The effects of psychological distance on abstraction: Two meta-analyses. *Psychological Bulletin*, 141, 525-548. doi.org/10.1037/bul0000005
- Sooniste, T., Granhag, P. A., Knieps, M., & Vrij, A. (2013). True and false intentions: Asking about the past to detect lies about the future. *Psychology, Crime & Law*, 19, 673-685. doi.org/10.1080/1068316X.2013.793333
- Sooniste, T., Granhag, P. A., Strömwall, L. A., & Vrij, A. (2014). Discriminating between true and false intent among small cells of suspects. *Legal and Criminological Psychology*, 21, 344-357. doi.org/10.1111/lcrp.12063
- Sooniste, T., Granhag, P. A., Strömwall, L. A., & Vrij, A. (2015). Statements about true and false intentions: Using the Cognitive Interview to magnify the differences. *Scandinavian Journal of Psychology*, 56, 371-378. doi.org/10.1111/sjop.12216
- Strömwall, L. A., Hartwig, M., & Granhag, P. A. (2006). To act truthfully: Nonverbal behavior and strategies during a police interrogation. *Psychology, Crime & Law*, 12, 207-219. doi: 10.1080/10683160512331331328
- Szpunar, K. K. (2010). Episodic future thought: An emerging concept. *Perspectives on Psychological Science*, 5, 142-162. doi: 10.1177/1745691610362350
- Taylor, P. J., Dando, C. J., Ormerod, T. C., Ball, L. J., Jenkins, M. C., Sandham, A., & Menacere, T. (2013). Detecting insider threats through language change. *Law and Human Behavior*, 37, 267-275. https://doi.org/10.1037/lhb0000032
- Toliver, R. F. (1997). *The interrogator: the story of Hans Joachim Scharff, master interrogator of the Luftwaffe*. Atglen, PA: Schiffer Publishing Ltd.
- Trope, Y., & Liberman, N. (2010). Construal-level theory of psychological distance. *Psychological Review*, 117, 440-463. doi.org/10.1037/a0018963
- Ulery, B. T., Hicklin, R. A., Buscaglia, J., & Roberts, M. A. (2012). Repeatability and reproducibility of decisions by latent fingerprint examiners. *PloS ONE*, 7. doi.org/10.1371/journal.pone.0032800

- Vallacher, R. R., & Wegner, D. M. (1987). What do people think they're doing? Action identification and human behavior. *Psychological Review*, 94, 3-15. doi.org/10.1037/0033-295X.94.1.3
- Van der Meer, B. B., & Diekhuis, M. L. (2014). Collecting and assessing information for threat assessment. In J. R. Meloy & J. Hoffmann (Eds.), *International handbook of threat assessment* (pp. 54-66). New York, NY: Oxford University Press.
- Vecchi, G. M., van Hasselt, V. B., & Romano, S. J. (2005). Crisis (hostage) negotiation: Current strategies and issues in high-risk conflict resolution. *Aggression and Violent Behavior*, 10, 533-551. doi.org/10.1016/j.avb.2004.10.001
- Vossekuil, B., Fein, R. A., & Berglund, J. M. (2015). Threat assessment: Assessing the risk of targeted violence. *Journal of Threat Assessment and Management*, 2, 243-254. doi.org/10.1037/tam0000055
- Vrij, A. (2008). Individual verbal cues to deception. *Detecting lies and deceit: Pitfalls and opportunities*. Chichester, UK: John Wiley & Sons.
- Vrij, A., Fisher, R., Mann, S., & Leal, S. (2008). A cognitive load approach to lie detection. *Journal of Investigative Psychology and Offender Profiling*, 5(1-2), 39-43. doi.org/10.1002/jip.82
- Vrij, A., & Granhag, P. A. (2014). Eliciting information and detecting lies in intelligence interviewing: An overview of recent research. *Applied Cognitive Psychology*, 28, 936-944. doi.org/10.1002/acp.3071
- Vrij, A., Granhag, P. A., Mann, S., & Leal, S. (2011a). Lying about flying: The first experiment to detect false intent. *Psychology, Crime & Law*, 17(7), 611-620. doi.org/10.1080/10683160903418213
- Vrij, A., Leal, S., Granhag, P. A., Mann, S., Fisher, R. P., Hillman, J., & Sperry, K. (2009). Outsmarting the liars: The benefit of asking unanticipated questions. *Law and Human Behavior*, 33, 159-166. doi: 10.1007/s10979-008-9143-y
- Vrij, A., Leal, S., Mann, S. A., & Granhag, P. A. (2011b). A comparison between lying about intentions and past activities: Verbal cues and detection accuracy. *Applied Cognitive Psychology*, 25, 212-218. doi.org/10.1002/acp.1665
- Wakslak, C. J., Trope, Y., Liberman, N., & Alony, R. (2006). Seeing the forest when entry is unlikely: probability and the mental representation of events. *Journal of Experimental Psychology: General*, 135, 641-653. doi: 10.1037/0096-3445.135.4.641

- Warren, L., Mullen, P., & McEwan, T. (2014). Explicit threats of violence. In J. R. Meloy & J. Hoffmann (Eds.), *International handbook of threat assessment* (pp. 18-38). New York, NY: Oxford University Press.
- Weber, E. U. (2001). Decision and choice: Risk, empirical studies. In N. J. Smelser & B. Baltes (Eds.), *International encyclopedia of the social and behavioral sciences*. (pp. 13347-13351). Amsterdam, NL: Elsevier. doi.org/10.1016/b0-08-043076-7/00634-3
- Wells, S. (2015). Hostage negotiation and communication skills in a terrorist environment. In J. Pearse (Ed.), *Investigating terrorism: Current political, legal and psychological issues* (pp. 144-166). Malden, MA: John Wiley & Sons.
- White, S. (2014). Workplace targeted violence: Threat assessment incorporating a structured professional judgment guide. In J. R. Meloy & J. Hoffmann (Eds.), *International handbook of threat assessment* (pp. 83-106). New York, NY: Oxford University Press.
- White, S. G., & Meloy, J. R. (2010). The WAVR-21: A structured professional guide for the workplace assessment of violence risk. *San Diego: Specialised Training Services*.
- Wright, M. (2013). Homicide detectives' intuition. *Journal of Investigative Psychology and Offender Profiling*, 10, 182-199. doi.org/10.1002/jip.1383
- Yang, M., Wong, S. C., & Coid, J. (2010). The efficacy of violence prediction: a meta-analytic comparison of nine risk assessment tools. *Psychological Bulletin*, 136, 740-767. doi: 10.1037/a0020473.

APPENDICES

Appendix A: Favourable ethical opinion (Study I & Study II)



GÖTEBORGS UNIVERSITET
Psykologiska institutionen

GÖTEBORG UNIVERSITY, *Department of Psychology*

Gothenburg, Sweden, February 11, 2016

To whom it may concern,

This letter concerns the two studies carried out by doctoral student Renate Geurts at University of Gothenburg (Department of Psychology) to be included in her PhD thesis.

Title of studies:

Study 1: Taking Threats to the Lab: Introducing an Experimental Paradigm for Studying Communicated Threats

Study 2: Communicated Threats: Strategies of Bluffers and Actualisers Examined

We have been running structurally similar studies at the Psychology Department for 15 years (40+ individual studies), using – more or less- the same paradigm and experimental setup. The Regional Ethical Review Board has explicitly and repeatedly informed us that we do not have to run each study (using this paradigm) via them. For those occasions where we submitted an application for a singular study, they have just returned the application with the response “We have received your application, but this study is not necessary to run through the Ethics Board”.

I attach one such statement from the Regional Ethics Board (unfortunately these statements only come in Swedish). This particular example regards a study where we examined the Scharff-technique (2012); importantly, in terms of structure, participants, instructions, interviews etc this study is very similar to the studies that have been carried out for Renate Geurts’ PhD (with me as her main supervisor).

Sincerely,

Pär Anders Granhag, PhD
Professor of Psychology
Director of the unit Criminal, Legal & Investigative Psychology (CLIP)

University of Gothenburg
Department of psychology
P.O. Box 500
405 30 Gothenburg
Sweden

pag@psy.gu.se
+46 (0)31 786 1647 (office)
+46 (0)733 107 297 (mobile)

Postadress
Box 500
.....direktval
405 30 GÖTEBORG

Besöksadress
Haraldsgatan 1
Göteborg

Telefon
031-773 10 00 Vx
Int +46 31 773 10 00
Fax No +46 31 773 46 28

Appendix B: Favourable ethical opinion (Study III)



GÖTEBORGS UNIVERSITET
Psykologiska institutionen

GÖTEBORG UNIVERSITY, Department of Psychology

Gothenburg, Sweden, September 1, 2016

To whom it may concern,

This letter concerns a study carried out by doctoral student Renate Guerts at University of Gothenburg (Department of Psychology) to be included in her PhD thesis.

Title of study:

Interviewing to Manage Threats: Exploring the Effects of Interview Style on Information Gain and Threateners' Counter-Interview Strategies

We have been running structurally similar studies at the Psychology Department for 15 years (40+ individual studies), using – more or less- the same paradigm and experimental setup. The Regional Ethical Review Board has explicitly and repeatedly informed us that we do not have to run each study (using this paradigm) via them. For those occasions where we submitted an application for a singular study, they have just returned the application with the response “We have received your application, but this study is not necessary to run through the Ethics Board”.

I attach one such statement from the Regional Ethics Board (unfortunately these statements only come in Swedish). This particular example regards a study where we examined the Scharff-technique (2012); importantly, in terms of structure, participants, instructions, interviews etc this study is very similar to the studies that have been carried out for Renate Guerts's PhD (with me as her main supervisor).

Sincerely,

Pär Anders Granhag, PhD

Professor of Psychology

Director of the unit Criminal, Legal & Investigative Psychology (CLIP)

University of Gothenburg
Department of psychology
P.O. Box 500
405 30 Gothenburg
Sweden

pag@psy.gu.se

+46 (0)31 786 1647 (office)

+46 (0)733 107 297 (mobile)

Postadress

Box 500

.....direktval

405 30 GÖTEBORG

Besöksadress

Haraldsgatan 1

Göteborg

Telefon

031-773 10 00 Vx

Int +46 31 773 10 00

Fax No +46 31 773 46 28

Appendix C: Favourable ethical opinion (Study IV)



Renate Geurts
Department of Psychology
University of Portsmouth

renate.geurts@psy.gu.se

Science Faculty Ethics Committee

Science Faculty Office
University of Portsmouth
St Michael's Building
White Swan Road
PORTSMOUTH
PO1 2DT

T: 023 9284 3379
ethics-sci@port.ac.uk

24th November 2015

FAVOURABLE ETHICAL OPINION WITH MINOR CONDITIONS

Study Title: **What is on in the field of threat assessment?**
Reference Number: **SFEC 2015-093** (Please quote this in any correspondence)

Thank you for submitting your application to the Science Faculty Ethics Committee (SFEC) dated 11/11/15 in accordance with current procedures¹.

I am pleased to inform you that SFEC was content to grant a favourable ethical opinion of the above research on the basis described in the submitted documents listed at Annex A, and subject to standard general conditions² and the following minor conditions/recommendations:

1. Please could the researcher refer to the University's consent form guidance and ensure all relevant points are covered in their consent form:
<http://www.port.ac.uk/research/ethics/downloads/filetodownload.171748.en.doc>

There is no requirement for you to confirm these conditions have been met in writing to the committee.

Please note that the favourable opinion of SFEC does not grant permission or approval to undertake the research. Management permission or approval must be obtained from any host organisation, including the University of Portsmouth or supervisor, prior to the start of the study.

Wishing you every success in your research

Yours sincerely,

Dr Simon Kolstoe
Alternate Vice Chair Science Faculty Ethics Committee

¹ Procedures for Ethical Review, Science Faculty Ethics Committee, University of Portsmouth, October 2012 (to be updated).

² After ethical review – Guidance for researchers (Please read).

Appendix D: Form UPR16

FORM UPR16**Research Ethics Review Checklist**

Please include this completed form as an appendix to your thesis (see the Postgraduate Research Student Handbook for more information)

Postgraduate Research Student (PGRS) Information		Student ID:	754991
PGRS Name:	RENATE GEURTS		
Department:	PSYCHOLOGY	First Supervisor:	PROF. ALDERT VRIJ
Start Date: (or progression date for Prof Doc students)	1 SEPTEMBER 2014		
Study Mode and Route:	Part-time <input type="checkbox"/> Full-time <input checked="" type="checkbox"/>	MPhil <input type="checkbox"/> PhD <input checked="" type="checkbox"/>	MD <input type="checkbox"/> Professional Doctorate <input type="checkbox"/>
Title of Thesis:	INTERVIEWING TO ASSESS AND MANAGE THREATS OF VIOLENCE		
Thesis Word Count: (excluding ancillary data)	33.254 words (excluding appendices)		
<p>If you are unsure about any of the following, please contact the local representative on your Faculty Ethics Committee for advice. Please note that it is your responsibility to follow the University's Ethics Policy and any relevant University, academic or professional guidelines in the conduct of your study</p> <p>Although the Ethics Committee may have given your study a favourable opinion, the final responsibility for the ethical conduct of this work lies with the researcher(s).</p>			
UKRIO Finished Research Checklist: (If you would like to know more about the checklist, please see your Faculty or Departmental Ethics Committee rep or see the online version of the full checklist at: http://www.ukrio.org/what-we-do/code-of-practice-for-research/)			
a) Have all of your research and findings been reported accurately, honestly and within a reasonable time frame?	YES NO	<input checked="" type="checkbox"/> <input type="checkbox"/>	
b) Have all contributions to knowledge been acknowledged?	YES NO	<input checked="" type="checkbox"/> <input type="checkbox"/>	
c) Have you complied with all agreements relating to intellectual property, publication and authorship?	YES NO	<input checked="" type="checkbox"/> <input type="checkbox"/>	
d) Has your research data been retained in a secure and accessible form and will it remain so for the required duration?	YES NO	<input checked="" type="checkbox"/> <input type="checkbox"/>	
e) Does your research comply with all legal, ethical, and contractual requirements?	YES NO	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Candidate Statement:			
I have considered the ethical dimensions of the above named research project, and have successfully obtained the necessary ethical approval(s)			
Ethical review number(s) from Faculty Ethics Committee (or from NRES/SCREC):		SFEC 2015-093	
If you have <i>not</i> submitted your work for ethical review, and/or you have answered 'No' to one or more of questions a) to e), please explain below why this is so:			
STUDY I, II, AND III HAVE BEEN APPROVED BY THE REGIONAL ETHICAL REVIEW BOARD OF GOTHENBURG UNIVERSITY (SEE APPENDICES A AND B)			

Signed (PGRS):		Date: 13 JULY 2017
----------------	---	--------------------

Appendix E: Manuscript Study I

Journal of Threat Assessment and Management
2016, Vol. 3, No. 1, 53–64

© 2016 American Psychological Association
2169-4842/16/\$12.00 <http://dx.doi.org/10.1037/tam0000060>

Taking Threats to the Lab: Introducing an Experimental Paradigm for Studying Verbal Threats

Renate Geurts

University of Gothenburg and University of
Portsmouth

Pär Anders Granhag

University of Gothenburg and Norwegian Police
University College

Karl Ask

University of Gothenburg

Aldert Vrij

University of Portsmouth

People who threaten to cause harm may either actualize their threat or bluff. To manage the risk that harmful acts will be perpetrated, it is of great importance to recognize differences between threatening behavior that will and will not be actualized. In this article we present what is, to our knowledge, the first study in which verbal threats are examined experimentally. We theorized that threats reflecting actual intentions come with implementation details (*how* one will actualize the threat), whereas bluffs linger in the formation of ideas (reasons *why* one makes a threat). In a mock-paradigm, participants ($N = 181$) threatened a company over the phone and were questioned about their threat during the call. Participants were either instructed not to actualize the threat (bluffers), to actualize it only if the company would not meet their demands (conditional actualizers) or to always actualize the threat (decisive actualizers). It was found that bluffers and actualizers differed in the amount of implementation details they provided. In contrast to our prediction, bluffers provided comparatively more details on implementation. Possible explanations for this result are discussed.

Keywords: threat assessment, true and false intent, construal level theory, investigative interviewing

On August 15, 1998, a car bomb exploded in the shopping center of Omagh, Northern Ireland. The explosion killed 29 people and injured another 220. The Real Irish Republican Army (Real IRA), a splinter group of the IRA, claimed responsibility for the attack. It was the deadliest attack in the Northern Ireland conflict. Strikingly, a warning preceded the bombing. Half an hour before the explosion a man called the Irish TV station and stated: “Martha Pope, bomb,

Omagh town, 15 minutes.” At the time, the Real IRA used the code “Martha Pope” when warning the police in order to distinguish themselves from those who threatened with fake attacks impersonating the IRA. In the Omagh-case the perpetrators thus explicitly revealed their true intentions. However, usually, the receiver does not know whether or not the threatener will do harm. Hence, threats come with great uncertainty (Meloy, Hart, & Hoffmann, 2013a). To assess potential risks, it is important to detect markers of actual threats and bluffs.

An actual threat is defined as a stated intention to cause harm that the threatener genuinely intends to carry out. We call people who express such threats *actualizers*. In contrast, a bluff is a stated intention to cause harm that the threatener does not intend to carry out. We call people who express such threats *bluffers*. In the present article we introduce a paradigm to study threats experimentally. Using this paradigm we examine whether, and if so how, intentions to

Renate Geurts, Department of Psychology, University of Gothenburg, and Department of Psychology, University of Portsmouth; Pär Anders Granhag, Department of Psychology, University of Gothenburg, and Department of Psychology, Norwegian Police University College; Karl Ask, Department of Psychology, University of Gothenburg; Aldert Vrij, Department of Psychology, University of Portsmouth.

Correspondence concerning this article should be addressed to Renate Geurts, Department of Psychology, University of Gothenburg, P. O. Box 500, 405 30 Gothenburg, Sweden. E-mail: renate.geurts@psy.gu.se

actualize threats manifest in the verbal content of threats. In other words, do actualizers verbalize themselves differently than bluffers do?

Threat Assessments

The contemporary research on threats is dominated by case studies. Most of these studies identify warning behaviors or risk factors associated with (threats to commit) targeted violence (Meloy, Hoffmann, Roshdi, Glaz-Ocik, & Guldemann, 2013b). Targeted violence concerns incidents where the perpetrator selects a target prior to his violent attack (Fein, Vossekuil, & Holden, 1995). Examples of targeted violence are stalking, acts of terrorism, school shootings, or workplace violence. Warning behaviors and risk factors are markers that relate to, and in certain cases predict, targeted violence (Meloy & O'Toole, 2011). Factors found to increase the risk of violence committed by threateners are prior violence, substance abuse, limited education (specifically verbal skill deficits), untreated mental disorders, and hostile/suspicious interaction styles (Warren, Mullen, & Ogloff, 2011; Warren, Ogloff, & Mullen, 2013). These predictors largely resemble the risk factors that are common to non-threatening perpetrators of violence (Yang, Wong, & Coid, 2010).

In addition to these general and clinical characteristics, specific risk factors have been identified for separate domains of targeted violence. Directly communicated threats, for instance, have been found to be a rather robust predictor of violence in cases of stalking (Mullen et al., 2006), whereas many school shooters have been found to reveal their violent plans indirectly to a third party (e.g., friend, classmate) prior to the attack (i.e., *leakage*; O'Toole, 2000). Furthermore, psychotic symptoms such as delusional beliefs and disordered communication are strongly associated with persons who threaten and attack royal figures, politicians, and celebrities (Dietz et al., 1991; James et al., 2007, 2008). Especially persons with intense preoccupations with an individual, activity or idea, appear to be overrepresented in statistics on the harassment of public figures (i.e., *fixation*; Hoffmann, 2009). Actual attacks of public figures are often preceded by approaches in the form of inappropriate letters or visits (James, Farnham, & Wilson, 2013). Other suggested warning be-

haviors are acts of planning and preparation (Calhoun & Weston, 2003), identification with military and weapons (Hempel, Meloy, & Richards, 1999), and an increase in attempts to pursue the objective (i.e., *intensity of pursuit*; Hoffmann, Meloy, & Sheridan, 2013). For an overview of warning behaviors, see Meloy and colleagues (2013b).

Two prominent insights have emerged from the work reviewed above. First, the likelihood of actualizing a threat of violence appears to be dependent on the situation and circumstances, rather than on the threatener's personality (Borum, Fein, Vossekuil, & Berglund, 1999). Second, most attacks are of a deliberate nature (Borum et al., 1999). Perpetrators form ideas, calculate, plan, prepare, and try out along their way to actual violence. When such behaviors follow a sequential structure it is sometimes referred to as a *pathway to violence* (for specific stages along this pathway, see Calhoun & Weston, 2003). This concept illustrates that targeted violence is the result of elaborate processes rather than impulses. Recognizing pre-attack behavior in an early stage is key to assessing threats (Fein et al., 1995). The prevailing approach to threat assessment is therefore to monitor patterns of thinking and behavior of those individuals who come to the attention of professionals (Meloy et al., 2013a). However, this individualized approach rests mainly on research examining cases that have gone wrong. This begs the question: How many individuals with similar behavior never caused harm? The answer to this question is important for assigning diagnostic value to warning behaviors. Furthermore, cases are generally analyzed in hindsight, and the findings are *described* rather than *predicted* from theory. We therefore argue that experimental research is needed to identify discriminative markers of actual threats and bluffs and, if possible, to provide a theoretical framework which may accommodate previous findings.

Construal Level Theory

One theory that may be particularly relevant to understanding threats is the construal level theory (Trope & Liberman, 2010). CLT was originally developed to explain how people mentally represent past and future situations such as memories, speculations, or plans. These

mental representations are called construals. Construals vary in abstractness depending on the psychological distance to the self. Psychological distance is the subjective experience of something being close or far away from the self, the here, and the now (Trope & Liberman, 2010). An event is psychologically distant when it transcends one's immediate experience. That is, when the event is supposed to take place in the distant future, at a distant location, applies to other people, and/or is uncertain to happen. For instance, the seminar your friend might attend next year in Dubai is more psychologically distant than the seminar you will attend tomorrow in your hometown. The CLT holds that construals become more concrete as psychological distance to an event decreases and, as a consequence, affect peoples' thoughts and behavior in relation to that specific event (Trope, Liberman, & Wakslak, 2007). This hypothesis has been supported in numerous studies and the results seem robust across different types of psychological distance, settings, and samples (Soderberg, Callahan, Kochersberger, Amit, & Ledgerwood, 2015).

The key difference between actualizers and bluffers is that the former intend to carry out their threat, whereas the latter do not. Although there is no clear line between actualizers and bluffers in reality (e.g., some might not have made up their mind yet), the literature suggests that all threateners find themselves on a pathway between an idea to cause harm and the actual implementation (Calhoun & Weston, 2003; Fein & Vossekuil, 1997). Their position on this pathway can change over time and situation (Meloy et al., 2013b). For instance, a man who stalks his ex-wife and plans to set her house on fire might refrain from doing so when he gets a new girlfriend. Thus, threateners vary in their psychological distance to an attack. According to CLT, actualizers should have more concrete mind-sets compared with those who are indecisive or bluff. The question is then, how—if at all—does the level of mental abstraction manifest itself in verbal threatening behavior?

One possibility is that actualizers and bluffers value the *desirability* and *feasibility* of their threat differently. Desirability concerns the valence of an action's end state, whereas feasibility refers to the ease or difficulty of reaching the end state (Liberman & Trope, 1998). For exam-

ple, one's wish to live in a just world reflects desirability, whereas all actions taken to create a just world reflect feasibility. The distinction between desirability and feasibility corresponds with the distinction between "why" and "how" aspects of an event. These aspects have been examined in research on how people think about what they are doing, so-called action identification (Vallacher & Wegner, 1987). "How" aspects are concrete and specify *how* one will act ("I will disgrace the company's image by leaking sensitive information to the media"). "Why" aspects are more abstract and specify *why* one will act ("I will shame the company's image because they treat their employers badly"). It has been theorized that people generally prefer to describe activities in terms of "why," but shift to "how" descriptions when "why" information fails to guide subsequent action (Vallacher & Wegner, 1987). Specifically, research shows that people describe activities in more concrete, "how" related terms when these activities are soon to happen (Liberman & Trope, 1998) and/or more likely to occur (Wakslak, Trope, Liberman, & Alony, 2006). The role of "how" and "why" representations have also been examined in relation to true and false intent (Gollwitzer & Sheeran, 2006; MacGiolla, Granhag, & Liu-Jönsson, 2013; Sooniste, Granhag, Strömwall, & Vrij, 2014). These studies are of particular relevance for the current context since threats can be seen as a specific form of intent.

True and False Intent

Gollwitzer (1999) proposed that "how" thinking is crucial for achieving goals. He suggested that the mere act of goal setting ("I want to shame the image of the company") is not enough to realize the goal. People also need *if-then* plans that specify when, where, and how the goal should be realized ("If they don't change their policy immediately, I will contact the media and leak sensitive information"). Such *if-then* plans are called *implementation intentions* and can be seen as the operationalization of the desired outcome, the goal intention (Gollwitzer, 1999). Research shows that individuals who form implementation intentions more often initiate goal striving and achieve their goals (Gollwitzer & Sheeran, 2006). Furthermore, individuals who have no goal intention are unlikely to form implementation inten-

tions (Sheeran, Milne, Webb, & Gollwitzer, 2005). Implementation intentions might thus be unique for true intentions. To examine this hypothesis, Sooniste, Granhag, Strömwall, and Vrij (2014), instructed truth tellers to plan and carry out a neutral task (grocery shopping), whereas liars were told to plan and carry out a mock crime (hiding a USB in the shopping center). The latter group was further instructed to lie about their true intentions in case they were intercepted, and to use a cover story to withstand the interview. When questioned about their intentions, truth tellers provided more “how” information than liars, and liars provided more “why” information than truth tellers. These findings were replicated in a subsequent study using a similar paradigm (MacGiolla et al., 2013; see also Granhag & MacGiolla, 2014).

Although threats essentially reflect intent, the results from past research cannot be directly applied to threats. Threats differ from the type of intentions studied so far in at least four critical aspects. First, the truth (not the lie) reflects higher criminal involvement. That is, actualizers have criminal plans whereas bluffers have less malicious intentions. In previous studies on true and false intentions, liars typically held criminal plans and truth tellers were innocent. Second, threateners emphasize their harmful intentions, whereas suspects commonly downplay or hide past actions. Third, no threatener is completely innocent. Making a threat (even with no intention to act upon it) is already harmful and sometimes criminal, depending on the severity of the threat and national legislation. The distinction between innocence and guilt is thus less sharp than in earlier intention studies. Fourth, implementation intentions are typically examined in social-cognitive research as a condition that is either present or absent. This dichotomy might not hold for situations where intentions to implement violence may range from mild to moderate and strong intent. Hence, a new strand of research is needed to examine true and false intentions in relation to threats.

The Present Study

In the present study we examined how actualizers and bluffers verbalize threats. Participants were presented with a case involving a nongovernmental organization (NGO) and a clothing company, and were then asked to represent the NGO when making a threatening

phone call to the company. Participants were either instructed not to actualize their threat (*bluffers*), to actualize the threat only if the company would not agree to meet the participants’ conditions (*conditional actualizers*), or to actualize the threat no matter how the company would respond (*decisive actualizers*). A confederate answered the phone calls always using four different questions (see below).

The likelihood that an event will happen affects how people think and talk about it (Wakslak et al., 2006). Specifically, “how” representations of events become more prominent when events are more likely to happen, for instance, in near future plans (Liberman & Trope, 1998), true intentions (MacGiolla et al., 2013; Sooniste et al., 2014), and implementation intentions (Gollwitzer & Sheeran, 2006). The likelihood of actualizing the threat was therefore manipulated across the three experimental conditions: bluffers (low likelihood), conditional actualizers (medium likelihood), and decisive actualizers (high likelihood). It was predicted that decisive actualizers would provide the most “how” information during the threat calls, followed by conditional actualizers, with bluffers providing the least “how” information. Given Vallacher and Wegner’s (1987) theoretical notion that we are all sensitive to the larger meanings and reasons for what we are doing, no differences were expected with respect to the amount of “why” information disclosed.

Furthermore, interview tactics may affect how much and what type of information threateners provide. The questions asked during the phone call in the present study can be divided into two categories: information-seeking (e.g., *Can you please give me more information?*) and challenging (e.g., *How do I know that you are telling me the truth?*). No specific predictions were formulated for the effect of the specific questions on information disclosure, but the response patterns to the questions were examined for exploratory purposes.

Method

Participants and Design

One-hundred eighty-one students (128 women, 53 men; $M_{age} = 28.31$ years, $SD = 10.05$ years) at the University of Gothenburg (Sweden) participated in the study. Participants

were recruited via the university participant pool. This pool consists of both students and nonstudents who have signed up for participation in psychological research. Participants were approached via e-mail and asked to take part in a study on campaigning strategies used by nongovernmental organizations (NGO). They received a cinema ticket for participation (worth approximately €11). Participants were randomly assigned to one of three experimental conditions: bluffers, conditional actualizers, and decisive actualizers. Seven persons felt uncomfortable making a threat and withdrew from the study. Seventeen participants did not correctly follow the instruction to act or not to act on their threat. Eleven of these had misunderstood or forgot this part of the instruction, and six did not believe that they were truly supposed to follow through with the threat. Their scores were excluded from further analysis. A total of 157 participants thus remained: 54 bluffers, 51 conditional actualizers and, 52 decisive actualizers (108 women, 49 men; $M_{age} = 28.10$ years, $SD = 9.67$ years).

Procedure

Participants were tested individually. The same case was presented to all participants. This case reflected a moral conflict between a fictive NGO named Aweare and a fictive clothing company named Vera. Participants read how Aweare was dedicated to improving working conditions in low-wage countries and how Vera was known as being socially engaged in the local communities in the countries to which they outsource their production. Vera had recently released a commercial in which they drew attention to violence against women. Meanwhile, Aweare got hold of video recordings showing how Vera exploited women in factories in Cambodia. Aweare considered it to be hypocritical that Vera raised public awareness about violence against women while simultaneously exploiting them for their own profit. Aweare therefore decided to take action against Vera. Participants were instructed to imagine being part of Aweare and to represent Aweare in this action.

All participants were instructed to call a representative of Vera and to threaten that they would leak the video recordings with evidence of Vera's malpractice to a Swedish TV program

for investigative journalism, if the company would not withdraw their commercial from television. Participants were either instructed not to leak the recordings (bluffers), to leak the recordings only if the company would not agree to withdraw their commercial (conditional actualizers), or to leak the recordings no matter how the company would respond to their threat (decisive actualizers). All participants were left alone for 15 min to prepare for their task(s) and all had access to the same background materials. These materials included both "why" related information (e.g., visions of Aweare, working conditions in Cambodia) and "how" related information (e.g., delivery location for the recordings, name of the media contact).

Next, the participants called the representative of Vera. They were led to believe that the person on the other end was another participant instructed to play the role as the representative. In reality, however, the recipient of the call was a confederate, who responded to the threats in the exact same manner, using four different questions/prompts:

Question 1 (Q1): Hello, this is Caroline. I'm the head of public relations at Vera and I expected your call. You initiated this conversation, so please go ahead.

Question 2 (Q2): I'm not sure I fully understand what you mean; can you please give me more information?

Question 3 (Q3): How do I know that what you are telling me is true?

Question 4 (Q4): Is there anything else I should know about before ending the conversation?

Okay, let me think about this. Thank you for your input. Bye.

After the conversation, the experimenter informed the participants that the Vera representative thought they were bluffing and therefore decided to ignore the threat. They were then instructed to proceed with their task according to the instructions. Bluffers were supposed to do nothing, whereas both conditional and decisive actualizers were supposed to provide their media contact with a USB stick containing the video recordings. They were intercepted immediately after starting the implementation (e.g., put on their coat, walked toward the door).

Before the participants made the call, they rated nine statements on their involvement with the case (e.g., “I consider women rights and poverty reduction to be two of the most important priorities for NGO’s to focus on;” 1 = *strongly disagree*, 7 = *strongly agree*) and their motivation to perform their task (e.g., “I want Vera to believe that my threat is real;” 1 = *strongly disagree*, 7 = *strongly agree*) using Likert scales. After the call and the interception, the participants rated the clarity of the instructions (1 = *very difficult*, 7 = *very easy*), their satisfaction with the preparation time (1 = *not at all sufficient*, 7 = *very sufficient*), the amount of preparation time spent on preparing for the call (1 = *no time at all*, 5 = *all the time*), the amount of preparation time spent on preparing for the delivery (1 = *no time at all*, 5 = *all the time*) and the credibility of the set up (e.g., “To what extent did you believe that you would deliver the USB stick to a contact person;” 1 = *very unlikely*, 7 = *very likely*). Participants were then thoroughly debriefed, thanked and paid for their participation.

Codings and Data Preparation

All calls were transcribed verbatim and coding was conducted on these transcriptions. Two coders, blind to the conditions and the hypotheses, first identified “how” and “why” information in the background materials that participants had access to while preparing the call. The coders relied on Liberman and Trope’s (1998) distinction between desirability (why) and feasibility (how). All information that related to the operations of Vera, the operations of Aware, the released commercial, and human rights in general was identified as “why” information. All information that related to the video recordings, the delivery procedure, the delivery location, and the possibilities to successfully implement the threat via investigative journalism or Aware, was identified as “how” information. In total, 44 pieces of “why” information and 32 pieces of “how” information were identified in the background materials. Each transcript was then coded for the amount of unique pieces of “how” information (range: 32) and “why” information (range: 44). Each piece of information was counted only the first time it was mentioned by the participant and repetitions were thus not taken into account. To assess the

interrater reliability, one coder coded all the transcripts and the other coder coded 20% of the transcripts. The interrater agreement was 90% (Cohen’s $\kappa = .71$).

To explore at which point in time during the interview participants disclosed their information, a new dependent measure was computed for “how” and “why” information, respectively, using the following equation:

$$T_{av} = \frac{n_1(1) + n_2(2) + n_3(3) + n_4(4)}{N}$$

where T_{av} = the average time (within the interval ranging from Question 1 to 4) when the information was reported, n_i = the number of pieces of information revealed at the i th question, and N = the total number of pieces of information revealed across all four questions. The measure could thus range from 1 (*all information revealed at Q1*) to 4 (*all information revealed at Q4*).

Results

Self-Ratings

Self-ratings on 7-point Likert scales showed that the participants believed in the setup ($M = 4.96$, $SD = 1.07$), were involved with the case ($M = 5.59$, $SD = 0.77$), and were highly motivated to make a convincing threat ($M = 6.25$, $SD = 0.92$). Moreover, they did not find it overly difficult to comply with the instructions ($M = 4.99$, $SD = 1.47$), experienced sufficient time to prepare for their tasks ($M = 4.53$, $SD = 1.72$), which they had largely spent preparing for the threat call ($M = 4.26$, $SD = 0.79$, rated on a 5-point scale). Analysis of variance (ANOVA) revealed no significant differences between conditions on the above measures. The only prethreat measure that showed differences between the conditions was the reported time spent on preparing for the delivery of the USB stick, $F(2, 146) = 16.52$, $p < .001$, $\eta^2 = .18$. A post hoc test, using Bonferroni-corrected alpha levels, revealed that bluffers reported significantly less preparation time spent on the delivery ($M = 1.20$, $SD = 0.40$) compared with both conditional actualizers ($M = 1.98$, $SD = 0.98$, $p < .001$) and decisive actualizers ($M = 2.02$, $SD = 0.94$, $p < .001$). This finding can be seen

as an additional manipulation check, as bluffers were not supposed to deliver the USB stick. When participants were asked in the debriefing to express their thoughts about the study, a substantial part spontaneously mentioned that they were nervous to make the call (48%), that the task was demanding (34%), and that the set-up felt real (26%).

Hypothesis Testing

The distributions of both “how” and “why” scores were negatively skewed ($skewness_{how} = 0.70$, $SE = 0.19$; $skewness_{why} = 1.63$, $SE = 0.19$) and leptokurtic ($kurtosis_{how} = 0.64$, $SE = 0.39$; $kurtosis_{why} = 5.53$, $SE = 0.39$). Hence, we conducted nonparametric analyses to test our hypothesis. The descriptive statistics for each of the experimental groups are reported in Table 1 (top panel).

To test for the predicted trend across conditions, individual scores were ranked and analyzed using the Jonckheere test. A significant trend in the “how” data was found. However, the conditions were ranked in opposite direction to what was predicted. The highest group median was found for bluffers, followed by conditional actualizers and decisive actualizers, $J = 3300$, $z = -2.61$, $p = .009$, $r = -.21$. Thus, the group that was least likely to actualize the threat (bluffers), was found to provide the most “how” information. Follow-up analysis, using Mann–Whitney tests with a Bonferroni correction, showed that bluffers provided significantly

more “how” information during the threat call than did decisive actualizers, $U = 971$, $z = -2.75$, $p = .006$, $r = -.27$. No significant difference was found between bluffers and conditional actualizers ($U = 1162$, $z = -1.38$, $p = .167$, $r = -.13$) or between decisive and conditional actualizers ($U = 1166.5$, $z = -1.06$, $p = .290$, $r = -.10$). With regard to the amount of “why” information provided during the threat calls, no significant difference between conditions was found using the Kruskal–Wallis test, $\chi^2(2, N = 157) = 0.56$, $p = .76$, $\eta^2 = .00$.

Exploratory Analyses

To examine the point in time during the interview at which participants disclosed their information, we conducted a Kruskal–Wallis analysis on the average timing of information disclosure. To understand how this dependent measure was conducted, see Codings and Data Preparation section. Descriptive statistics are reported in Table 1 (bottom panel). The analysis revealed that the timing of disclosure of “how” information differed between the conditions, $\chi^2(2, N = 157) = 8.85$, $p = .012$, $\eta^2 = .06$. Pairwise Mann–Whitney comparisons, using Bonferroni-corrected alpha levels, revealed that bluffers disclosed “how” information significantly later in the interview than did decisive actualizers, $U = 944.5$, $z = -2.91$, $p = .004$, $r = -.28$. No significant differences were found between bluffers and conditional actualizers ($U = 1127$, $z = -1.60$, $p = .109$, $r = -.15$)

Table 1
Descriptive Statistics for the Amount (Top Panel) and Timing (Bottom Panel) of
“Why” and “How” Information Revealed by Bluffers, Conditional Actualizers,
and Decisive Actualizers

Condition	Why			How		
	<i>M</i> (<i>SD</i>)	95% CI	<i>Mdn</i>	<i>M</i> (<i>SD</i>)	95% CI	<i>Mdn</i>
Amount						
Bluffers	8.31 (3.29)	[7.42, 9.21]	8.00	8.80 (3.18)	[7.93, 9.66]	9.00
Conditional	8.18 (3.74)	[7.13, 9.23]	8.00	8.35 (4.07)	[7.21, 9.50]	7.00
Decisive	8.35 (4.86)	[6.99, 9.70]	7.00	7.25 (3.17)	[6.37, 8.13]	7.00
Time						
Bluffers	1.81 (.40)	[1.70, 1.92]	1.80	2.40 (.78)	[2.19, 2.62]	2.33
Conditional	1.58 (.45)	[1.46, 1.71]	1.50	2.17 (.74)	[1.97, 2.38]	2.10
Decisive	1.58 (.42)	[1.46, 1.70]	1.50	1.98 (.76)	[1.77, 2.19]	1.85

Note. The time variables correspond to the average point in time during the interview at which the information was revealed (1 = all information revealed at Question 1, 4 = all information revealed at Question 4).

and between conditional and decisive actualizers ($U = 1104$, $z = -1.47$, $p = .143$, $r = -.15$). A similar pattern was observed for the timing of “why” information. The point in time during the interview at which participants disclosed “why” information differed between conditions, $\chi^2(2, N = 157) = 11.58$, $p = .003$, $\eta^2 = .07$. Bluffers disclosed “why” information significant later in the interview than did conditional actualizers ($U = 917$, $z = -2.95$, $p = .003$, $r = -.29$) and decisive actualizers ($U = 943.5$, $z = -2.91$, $p = .004$, $r = -.28$). No significant difference was found between conditional and decisive actualizers ($U = 1346$, $z = .13$, $p = .895$, $r = .01$).

All interviews started with two information-seeking questions/prompts (Q1: “Please go ahead” and Q2: “Can you please give me more information”), followed by two challenging questions (Q3: “How do I know that what you are telling me is true?” and Q4: “Is there anything else I should know about before ending the conversation?”). The patterns of change in responses from the information-seeking phase (Q1 and Q2) to the challenging phase (Q3 and Q4) differed significantly between the experimental conditions. More specifically, 44% of the bluffers revealed more “how” information in the challenging phase than in the information-seeking phase, compared with 23% of the conditional actualizers, and 17% of the decisive actualizers, $\chi^2(2, N = 157) = 9.67$, $p = .008$, $\eta^2 = .06$. Again, pairwise comparisons only revealed significant differences between bluffers and decisive actualizers ($p = .007$, $r = .30$). No difference was found with respect to “why” information. Participants in all conditions showed similar patterns of change in their “why” response. Only 2% of the bluffers, 2% of the conditional actualizers, and 2% of the decisive actualizers revealed more “why” information in the challenging phase than in the information-seeking phase, $\chi^2(2, N = 157) = 0.35$, $p = .839$, $\eta^2 = .00$.

Discussion

Major Findings

We introduced a paradigm for studying threats using an experimental method and we reported the results of the very first study drawing on this new paradigm. The study provided some support for the hypothesis that actualizers and bluffers use “how” information differently

when they threaten. Opposite to the predicted direction, bluffers revealed more details on *how* they would implement their threat, compared to those who were truly determined to act. This difference became particularly pronounced when participants were challenged. That is, when they were critically questioned (“How do I know that what you are telling me is true?”) or given a last opportunity to talk (“Is there anything more I should know about before ending this conversation?”). Overall, bluffers revealed more information later in the interview compared with the actualizers. The combined findings indicate that bluffers (vs. actualizers) more often resort to “how” details when challenged. The results contradict previous studies in which detailed accounts on planning and implementation are generally associated with true intent (MacGiolla et al., 2013; Sooniste et al., 2014) and executing threats (Calhoun & Weston, 2003). The findings also conflict with the notion derived from the construal level theory that the more likely it is that an event will happen in the near future, the more concrete (“how” related) this event will be construed and described (Wakslak et al., 2006).

One explanation for the current results could be that the mental construals of threateners are overshadowed by strategic considerations. The hypotheses were based on the theoretical notion that people describe future plans in accordance with their mental representations of these plans. In other words, the more concrete the plans, the more concrete the descriptions of these plans. What we failed to consider, was how people choose to reveal or conceal information. Milburn and Watman (1981) proposed that threatening behavior is a social construct and that people rationally choose the content of threats in order to gain control in unpredictable situations. Hence, people might have deliberate ideas about *when* to provide *what* piece of information when they are questioned about threats. In other words, stated threats might be more colored by what is *best* to say, rather than what is *possible* to say. As a result, participants that intended to actualize their threat might have had more “how” details in mind compared to bluffing participants (as predicted in present study) but, more often than bluffers, chose to keep those details for themselves (as found in the present study).

This explanation finds support in the literature on suspect interviewing. It has been found that guilty and innocent suspects differ both with respect to the degree to which they apply strategies during interviews, and the type of strategies they report to use (Hartwig, Granhag, & Strömwall, 2007). Guilty suspects generally balance the risk of revealing incriminating details (Granhag & Hartwig, 2008) and tend to avoid to reveal information about criminal activities (Hartwig et al., 2007). Because the actualizing participants in the present study had intent to do harm, they might have adopted a guilty-suspect strategy. That is, withholding “how” details to prevent being exposed. Bluffers, on the other hand, might not have worried too much about a successful implementation of their threat. Instead, the interviewer’s perception of their truthfulness may have mattered more. As liars typically do not take their credibility for granted (Vrij, Fisher, Mann, & Leal, 2008), bluffers are likely to fear not being believed. Recent research shows that deceptive interviewees tend to alter their verbal strategies when they become aware of the possibility that there is evidence speaking to their guilt (Luke, Dawson, Hartwig, & Granhag, 2014; Tekin et al., 2015). This threat to their credibility makes them either very forthcoming or very withholding. Hence, similar credibility concerns might have caused the bluffing threateners in the present study to become more forthcoming as the interview became more critical.

Although we found significant differences with respect to verbal behavior of bluffers and decisive actualizers, the two groups did not differ from the conditional actualizers. This might have been due to our manipulation: The likelihood to *actualize* the threat (deliver USB stick) was manipulated between conditions. However, the likelihood to *make* the threat was the same for all three conditions (all participants had to make the phone call). Because participants were generally nervous for making the call and spent most of the preparation time preparing for this, less thoughts and effort might have gone to the actual manipulation (i.e., delivering the USB stick or not). If this was the case, the conditions did not differ too much from each other and we failed to manipulate the participants’ construals and subsequent behavior. To our defense, however, differences between bluffers and actualizers might be small in real life too. Making a

threat is probably demanding and nerve-racking regardless of the intention to follow it through or not. Differently put, if the mere act of threatening affects bluffers and actualizers to a similar extent, they might not differ markedly at first sight. Traditional deception research shows that people behave very similarly when lying and when telling the truth (Bond & DePaulo, 2006). Hence, several lie-detection researchers now advocate developing interview techniques that elicit and enhance cues to deceit, rather than assuming that cues are present at face value (Vrij & Granhag, 2012). The same reasoning might apply to research on threats.

Further Research

The results of the present study cannot test the abovementioned assumptions on counter-interview strategies of threateners. Hence, further research is needed to explore these theoretical notions. Interview tactics that challenge the threatener’s credibility, or interfere with successful implementation, might magnify differences in verbal behavior between actualizers and bluffers. Interviewing to elicit and enhance cues to deception is viewed as a promising strand of research (Vrij & Granhag, 2012). However, when applying traditional deception detection strategies to threats, a different interplay between interviewer and interviewee might arise. Key concepts such as guilt, innocence, truth, and lies are cross-paired within threateners. In other words, threateners are either innocent liars or guilty truth tellers. This is different from the typical lie detection paradigm in which the truth teller is innocent and the liar is guilty.

Aside from interview tactics that may assist risk assessment, future research should also focus on interview tactics that may effectuate de-escalation. Today, threat assessment interviewing is primarily focused on information gathering, specifically, on the identification of risk factors (Van der Meer & Diekhuis, 2013). However, research on reoffending supports the view that violence risk is best managed when controlling for risk factors *and* when focusing on fulfilling the personal needs of the offender, for instance to arrange work that they enjoy (Andrews, Bonta, & Wormith, 2011). Such a combined approach is arguably relevant to the field of threat assessment as ignored desires (or at least desires experienced by the threatener as

being ignored) often grounds threatening behavior (Calhoun & Weston, 2003). Ideally, the threat assessment interview offers an opportunity to reach out to the subject of concern. The importance of stabilizing the situation and creating a fruitful interview climate has been acknowledged in the field of threat assessment (Van der Meer & Diekhuis, 2013). However, evidence-based interview tactics to arrive at these conditions are currently lacking. Future research may profit from developing interview tactics that combine (a) the aim to gather information and (b) the aim to de-escalate the threat.

Generalizability and Practical Applications

The generalizability of the current findings might be limited by the overrepresentation of females in the tested sample. This ratio contrasts the samples in previous case studies where the threats were almost always made by males (e.g., Warren et al., 2011). As the case studies relied on actual data, the overrepresentation of males in the studied samples plausibly reflects a gender asymmetry in the underlying population. It is therefore recommended to include more male participants in future experimental studies on threats.

A second limitation for the generalization of the findings is the limited personal involvement in the threats made. Although participants in the current study reported that they felt involved in the case, that they were motivated to perform well, and that they experienced participation as real and demanding, an experimental setting remains artificial. Such setting obviously differs from the more complex circumstances in which threatening behavior commonly occurs (e.g., hostile world views, untreated mental illness, intense preoccupations; Warren et al., 2013). However, an exact resemblance of the real-world is not always needed to gain insight into a phenomenon (Mook, 1983). The experimental paradigm allowed us to examine the basic characteristics in statements of persons who threaten. Moreover, such a setting creates the opportunity to investigate what can be made to occur. That is, what can be said or done by a threat assessor to elicit more information from a subject of concern. This knowledge could then be used to develop interview tactics for threat assessors. Strategic interviewing has proven to be beneficial in other areas of investigative interviewing. Tactics were developed that successfully elic-

ited cues to deceit in liars (Granhag & Hartwig, 2015), admissions from guilty suspects (Tekin et al., 2015) and information from sources who held knowledge about an upcoming crime (Oleszkiewicz, Granhag, & Montecinos, 2014). Thus, research on threat assessment interviewing may lead to protocols and tactics that help the threat assessor to elicit more, or more relevant, information.

Furthermore, a better understanding of the communication of threateners and their counterinterview strategies may shed new light on current concerns for interviewing them, such as the subjects' lack of insight into their own plans, their unwillingness to talk about their situation (Meloy et al., 2013a), and judicial or practical difficulties (Van der Meer & Diekhuis, 2013). However, before developing interview protocols for threat assessors, several protocols and tactics need to be tested under different conditions and in different contexts.

Conclusions

Taken together, this study is one of the first to address verbal threats experimentally. Its contribution is threefold; first, a new paradigm was presented in which the interaction between the threatener and the receiver could be examined. Although ecological concerns will always remain, this study showed that the basic aspects of threatening communication can be mirrored in a controlled setting. Second, our predictions were guided by theories on social cognition. Translating research from social cognition to threatening behavior could strengthen the theoretical base underlying the field of threat assessment (Milburn & Watman, 1981). Such a contribution should not be underestimated, considering that this field is currently short of theoretically driven predictions. Third, the results indicate that "how" information may be of diagnostic value when assessing statements expressing threats. We did not directly test the effects of different interview protocols on threateners' verbal behavior. However, our data suggest that differences between bluffers and actualizers may further increase as challenging questions are asked. This tendency could be the result of the threateners' strategic concerns. Future research should therefore address (a) what verbal strategies actualizers and bluffers adopt and (b) how different interview protocols (and tactics) may affect their strategies and verbal behavior.

References

- Andrews, D. A., Bonta, J., & Wormith, J. S. (2011). The risk-need-responsivity (RNR) model: Does adding the good lives model contribute to effective crime prevention? *Criminal Justice and Behavior*, 38, 735–755. <http://dx.doi.org/10.1177/0093854811406356>
- Bond, C. F., Jr., & DePaulo, B. M. (2006). Accuracy of deception judgments. *Personality and Social Psychology Review*, 10, 214–234. http://dx.doi.org/10.1207/s15327957pspr1003_2
- Borum, R., Fein, R., Vossekuil, B., & Berglund, J. (1999). Threat assessment: Defining an approach for evaluating risk of targeted violence. *Behavioral Sciences & the Law*, 17, 323–337. [http://dx.doi.org/10.1002/\(SICI\)1099-0798\(199907/09\)17:3<323::AID-BSL349>3.0.CO;2-G](http://dx.doi.org/10.1002/(SICI)1099-0798(199907/09)17:3<323::AID-BSL349>3.0.CO;2-G)
- Calhoun, F. S., & Weston, S. W. (2003). *Contemporary threat management: A practical guide for identifying, assessing, and managing individuals of violent intent*. San Diego, CA: Specialized Training Services.
- Dietz, P. E., Matthews, D. B., Van Duyne, C., Martell, D. A., Parry, C. D., Stewart, T., . . . Crowder, J. D. (1991). Threatening and otherwise inappropriate letters to Hollywood celebrities. *Journal of Forensic Sciences*, 36, 185–209.
- Fein, R. A., & Vossekuil, B. (1997). *Preventing assassination: Secret Service exceptional case study project*. Washington, DC: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.
- Fein, R. A., Vossekuil, B., & Holden, G. A. (1995). *Threat assessment: An approach to prevent targeted violence*, 2. Washington, DC: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.
- Gollwitzer, P. M. (1999). Implementation intentions: Strong effects of simple plans. *American Psychologist*, 54, 493–503. <http://dx.doi.org/10.1037/0003-066X.54.7.493>
- Gollwitzer, P. M., & Sheeran, P. (2006). Implementation intentions and goal achievement: A meta-analysis of effects and processes. *Advances in Experimental Social Psychology*, 38, 69–119. [http://dx.doi.org/10.1016/S0065-2601\(06\)38002-1](http://dx.doi.org/10.1016/S0065-2601(06)38002-1)
- Granhag, P. A., & Hartwig, M. (2008). A new theoretical perspective on deception detection: On the psychology of instrumental mind-reading. *Psychology, Crime & Law*, 14, 189–200. <http://dx.doi.org/10.1080/10683160701645181>
- Granhag, P. A., & Hartwig, M. (2015). The strategic use of evidence (SUE) technique: A conceptual overview. In P. A. Granhag, A. Vrij, & B. Verschuere (Eds.), *Deception detection: Current challenges and cognitive approaches* (pp. 231–251). London, UK: Wiley Blackwell.
- Granhag, P. A., & MacGiolla, E. (2014). Preventing future crimes. *European Psychologist*, 19, 195–206. <http://dx.doi.org/10.1027/1016-9040/a000202>
- Hartwig, M., Granhag, P. A., & Strömwall, L. A. (2007). Guilty and innocent suspects' strategies during police interrogations. *Psychology, Crime & Law*, 13, 213–227. <http://dx.doi.org/10.1080/10683160600750264>
- Hempel, A. G., Meloy, J. R., & Richards, T. C. (1999). Offender and offense characteristics of a nonrandom sample of mass murderers. *Journal of the American Academy of Psychiatry and the Law Online*, 27, 213–225.
- Hoffmann, J. (2009). Public figures and stalking in the European context. *European Journal on Criminal Policy and Research*, 15, 293–305. <http://dx.doi.org/10.1007/s10610-009-9104-0>
- Hoffmann, J. E. N. S., Meloy, J. R., & Sheridan, L. (2013). Contemporary research on stalking, threatening, and attacking public figures. In J. R. Meloy & J. Hoffmann (Eds.), *International handbook of threat assessment* (pp. 160–177). New York, NY: Oxford University Press.
- James, D. V., Farnham, F. R., & Wilson, S. P. (2013). The fixated threat assessment center: Implementing a joint policing and psychiatric approach to risk assessment and management in public figure threat cases. In J. R. Meloy & J. Hoffmann (Eds.), *International handbook of threat assessment* (pp. 299–320). New York, NY: Oxford University Press.
- James, D. V., Mullen, P. E., Meloy, J. R., Pathé, M. T., Farnham, F. R., Preston, L., & Darnley, B. (2007). The role of mental disorder in attacks on European politicians 1990–2004. *Acta Psychiatrica Scandinavica*, 116, 334–344. <http://dx.doi.org/10.1111/j.1600-0447.2007.01077.x>
- James, D. V., Mullen, P. E., Pathé, M. T., Meloy, J. R., Farnham, F. R., Preston, L., & Darnley, B. (2008). Attacks on the British Royal family: The role of psychotic illness. *Journal of the American Academy of Psychiatry and the Law Online*, 36, 59–67.
- Lieberman, N., & Trope, Y. (1998). The role of feasibility and desirability considerations in near and distant future decisions: A test of temporal construal theory. *Journal of Personality and Social Psychology*, 75, 5–18. <http://dx.doi.org/10.1037/0022-3514.75.1.5>
- Luke, T. J., Dawson, E., Hartwig, M., & Granhag, P. A. (2014). How awareness of possible evidence induces forthcoming counter-interrogation strategies. *Applied Cognitive Psychology*, 28, 876–882. <http://dx.doi.org/10.1002/acp.3019>
- Mac Giolla, E., Granhag, P. A., & Liu-Jönsson, M. (2013). Markers of good planning behavior as a cue for separating true and false intent. *PsyCh Journal*, 2, 183–189. <http://dx.doi.org/10.1002/pchj.36>

- Meloy, J. R., Hart, S. D., & Hoffmann, J. (2013a). Threat assessment and threat management. In J. R. Meloy & J. Hoffmann (Eds.), *International handbook of threat assessment* (pp. 3–17). New York, NY: Oxford University Press.
- Meloy, J. R., Hoffmann, J., Roshdi, K., Glaz-Ocik, J., & Guldinann, A. (2013b). Warning behaviors and their configurations across various domains of targeted violence. In J. R. Meloy & J. Hoffmann (Eds.), *International handbook of threat assessment* (pp. 39–53). New York, NY: Oxford University Press.
- Meloy, J. R., & O'Toole, M. E. (2011). The concept of leakage in threat assessment. *Behavioral Sciences & the Law*, 29, 513–527. <http://dx.doi.org/10.1002/bsl.986>
- Milburn, T. W., & Watman, K. H. (1981). *On the nature of threat: A social psychological analysis*. New York, NY: Praeger.
- Mook, D. G. (1983). In defense of external invalidity. *American Psychologist*, 38, 379–387. <http://dx.doi.org/10.1037/0003-066X.38.4.379>
- Mullen, P. E., Mackenzie, R., Ogloff, J. R., Pathé, M., McEwan, T., & Purcell, R. (2006). Assessing and managing the risks in the stalking situation. *Journal of the American Academy of Psychiatry and the Law Online*, 34, 439–450.
- Oleszkiewicz, S., Granhag, P. A., & Montecinos, S. C. (2014). The Scharff-technique: Eliciting intelligence from human sources. *Law and Human Behavior*, 38, 478–489. <http://dx.doi.org/10.1037/lhb0000085>
- O'Toole, M. E. (2000). *The school shooter: A threat assessment perspective*. Washington, DC: Department of Justice, Federal Bureau of Investigations.
- Sheeran, P., Milne, S., Webb, T. L., & Gollwitzer, P. M. (2005). Implementation intentions and health behavior. In M. Conner & P. Norman (Eds.), *Predicting Health Behavior: Research and Practice with Social Cognition Models* (pp. 276–323). Milton Keynes, UK: Open University Press.
- Soderberg, C. K., Callahan, S. P., Kochersberger, A. O., Amit, E., & Ledgerwood, A. (2015). The effects of psychological distance on abstraction: Two meta-analyses. *Psychological Bulletin*, 141, 525–548. <http://dx.doi.org/10.1037/bul0000005>
- Sooniste, T., Granhag, P. A., Strömwall, L. A., & Vrij, A. (2014). Discriminating between true and false intent among small cells of suspects. *Legal and Criminological Psychology*. Advance online publication. <http://dx.doi.org/10.1111/lcrp.12063>
- Tekin, S., Granhag, P. A., Strömwall, L., Giolla, E. M., Vrij, A., & Hartwig, M. (2015). Interviewing strategically to elicit admissions from guilty suspects. *Law and Human Behavior*, 39, 244–252. <http://dx.doi.org/10.1037/lhb0000131>
- Trope, Y., & Liberman, N. (2010). Construal-level theory of psychological distance. *Psychological Review*, 117, 440–463. <http://dx.doi.org/10.1037/a0018963>
- Trope, Y., Liberman, N., & Wakslak, C. (2007). Construal levels and psychological distance: Effects on representation, prediction, evaluation, and behavior. *Journal of Consumer Psychology: The Official Journal of the Society for Consumer Psychology*, 17, 83–95. [http://dx.doi.org/10.1016/S1057-7408\(07\)70013-X](http://dx.doi.org/10.1016/S1057-7408(07)70013-X)
- Vallacher, R. R., & Wegner, D. M. (1987). What do people think they're doing? Action identification and human behavior. *Psychological Review*, 94, 3–15. <http://dx.doi.org/10.1037/0033-295X.94.1.3>
- Van der Meer, B. B., & Diekhuis, M. L. (2013). Collecting and assessing information for threat assessment. In J. R. Meloy & J. Hoffmann (Eds.), *International handbook of threat assessment* (pp. 54–66). New York, NY: Oxford University Press.
- Vrij, A., Fisher, R., Mann, S., & Leal, S. (2008). A cognitive load approach to lie detection. *Journal of Investigative Psychology and Offender Profiling*, 5, 39–43. <http://dx.doi.org/10.1002/jip.82>
- Vrij, A., & Granhag, P. A. (2012). Eliciting cues to deception and truth: What matters are the questions asked. *Journal of Applied Research in Memory & Cognition*, 1, 110–117. <http://dx.doi.org/10.1016/j.jarmac.2012.02.004>
- Wakslak, C. J., Trope, Y., Liberman, N., & Alony, R. (2006). Seeing the forest when entry is unlikely: Probability and the mental representation of events. *Journal of Experimental Psychology: General*, 135, 641–653. <http://dx.doi.org/10.1037/0096-3445.135.4.641>
- Warren, L. J., Mullen, P. E., & Ogloff, J. R. (2011). A clinical study of those who utter threats to kill. *Behavioral Sciences & the Law*, 29, 141–154. <http://dx.doi.org/10.1002/bsl.974>
- Warren, L. J., Ogloff, J. R., & Mullen, P. E. (2013). The psychological basis of threatening behavior. *Psychiatry, Psychology and Law*, 20, 329–343. <http://dx.doi.org/10.1080/13218719.2012.674716>
- Yang, M., Wong, S. C., & Coid, J. (2010). The efficacy of violence prediction: A meta-analytic comparison of nine risk assessment tools. *Psychological Bulletin*, 136, 740–767. <http://dx.doi.org/10.1037/a0020473>

Received November 26, 2015

Revision received April 5, 2016

Accepted April 6, 2016 ■

Appendix F: Manuscript Study II

Journal of Applied Research in Memory and Cognition 6 (2017) 158–166



Contents lists available at ScienceDirect

Journal of Applied Research in Memory and Cognition

journal homepage: www.elsevier.com/locate/jarmac

Empirical article

Eliciting Information from People Who Pose a Threat:
Counter-Interview Strategies Examined[☆]

Renate Geurts*

University of Gothenburg, Sweden
University of Portsmouth, United Kingdom

Karl Ask

University of Gothenburg, Sweden

Pär Anders Granhag

University of Gothenburg, Sweden
Norwegian Police University College, Norway

Aldert Vrij

University of Portsmouth, United Kingdom

Threat managers—who aim to identify potential danger—typically collect information from sources around persons who pose a threat rather than questioning the threateners themselves. To elicit valuable information from threateners, it is important to understand the strategies they use to withstand interviews (i.e., counter-interview strategies). In the experiment, participants ($N = 179$) communicated a threat that they intended to actualize (actualizers) or not (bluffers), and were subsequently questioned about the threat using an interview protocol intended to communicate high or low suspicion. The findings showed that threatening required self-regulation. Participants were forthcoming, yet strategic and adaptive to the targets' response. Actualizers provided fewer details on how to implement the threat than did bluffers, and, when subjected to follow-up questions bluffers increased the information provision more than did actualizers. Knowledge on counter-interview strategies of threateners may contribute to the development of interview protocols that can be used to assess risk for violence.

General Audience Summary

People who threaten to do harm, cause fear and—in some cases—they cause actual damage. To manage potential danger, threat managers need to collect information and identify risk factors. For instance, what is the threatener's intent? Does the threatener experience feelings of hopelessness? Does the threatener see violence as acceptable? Although these questions may best be answered by the threatener, threat managers rarely engage with him or her. Instead, sources *around* the threatener are typically inquired, such as a teacher, a colleague, medical records or police reports. In the present paper we argue that it is important to understand how to elicit valuable information from threateners, so that threat managers can profit from first-hand information.

Author Note

[☆] Please note that this paper was handled by the current editorial team of JARMAC.

* Correspondence concerning this article should be addressed to Renate Geurts, Department of Psychology, University of Gothenburg, P.O. Box 500, 405 30 Gothenburg, Sweden. Contact: renate.geurts@psy.gu.se

A first step in this direction was taken by examining how threateners verbally behave when being questioned. Specifically, when do they reveal (or conceal) what type of information, and why? The experiment took place in a laboratory where participants expressed a threat that they intended to actualize (*actualizers*) or not (*bluffers*). They were then questioned about the threat they had made. The results showed that although participants were eager to share information, they deliberately chose how to present the case and what information to emphasize. Actualizers were more forthcoming on own initiative, whereas bluffers provided more information when questioned. Furthermore, actualizers revealed less information than bluffers on how to implement the threat. Understanding how threateners respond in interview settings may help threat managers to elicit information directly from the threatener. Such information can be used to assess potential danger posed by the threatener and to arrange appropriate interventions.

Keywords: Threat assessment, Information elicitation, Counter-interview strategy, Investigative interviewing, True intent

Interpersonal threats imply that a person might cause harm to themselves or others. Such harm can be physical (e.g., murder), but also psychological (e.g., stalking), or financial (e.g., company shaming). As the future is unknown, threats come with great uncertainty. The person who knows most about the posed threat is the threatener him/herself, yet little is known about how to elicit information from people who threaten. The current study focusses on collecting information from threateners via interviewing. Their information can be of great value for threat managers who need to assess and manage the risk for harmful behavior. A problem may be, however, that threateners behave differently when they know they are being examined (Meloy, Hart, & Hoffmann, 2013). They might exaggerate or downplay their intentions and might conceal or lie about their plans. Such behaviors, aimed to withstand the interview, have previously been studied in research on suspect interviewing and are commonly referred to as *counter-interview strategies* (Granhag, Clemens, & Strömwall, 2009).

Understanding the counter-interview strategies of interviewees has proven to be beneficial in several areas of investigative interviewing. Techniques have been developed that successfully elicit cues to deceit in liars (Granhag & Hartwig, 2015), admissions from guilty suspects (Tekin et al., 2015), and information from sources who hold knowledge about an upcoming crime (Oleszkiewicz, Granhag, & Cancino Montecinos, 2014). The commonality in these techniques is that they are developed from the perspective of the interviewee. In this paper we argue that in order to elicit valuable information from threateners it is important to understand their verbal strategies used when being questioned. Studying counter-interview strategies reflects a new line of research in the field of threat assessment. An experimental paradigm was developed for this purpose.

Suspects' Counter-Interview Strategies

Research has shown that counter-interview strategies reflect self-regulation (Granhag & Hartwig, 2008; Granhag et al., 2015; Hartwig, Granhag, Strömwall, & Doering, 2010). This means that when suspects are interrogated, they regulate their behavior to make a credible impression. Research has shown that guilty and innocent suspects are equally motivated to be perceived as truthful (Hartwig et al., 2010). However, guilty suspects need to conceal the truth, while innocent suspects can freely reveal the truth. This difference is presumed to result in avoidant

versus forthcoming counter-interview strategies. It has been found that guilty suspects are more often concerned with maintaining control and more often adapt avoidant strategies (e.g., *avoid incriminating details, keep it simple*), whereas innocent suspects are more concerned with providing correct information and more often adapt forthcoming strategies (e.g., *tell the truth like it happened*; Hines et al., 2010; Strömwall, Hartwig, & Granhag, 2006). Furthermore, it has been found that guilty suspects use more, and more diverse strategies than innocent suspects (Hartwig, Granhag, & Strömwall, 2007), are more aware of the risk of not being believed (Hartwig et al., 2010), and react comparatively stronger to the possibility that there might be evidence against them (Luke, Dawson, Hartwig, & Granhag, 2014).

Threateners' Counter-Interview Strategies

A threat is ineffective if the target person does not believe the threat. Just like suspects, threateners thus need to be convincing. However, we suggest that threateners might use different counter-interview strategies than suspects of a crime. As it is difficult to be convincing by being avoidant, it is presumed that threateners—regardless of whether or not they bluff—need to be forthcoming. Complete honesty, however, is not possible. Those with no intent to actualize their plans need to conceal that they are bluffing, but those with the intent to enact their plans might want to conceal information that can cause interference with the implementation of their plan, such as the exact time or place for the attack. Although intentions may typically range from mild to moderate and strong intent, this paper distinguishes only between the presence and absence of implementation intentions.

Information on how to implement the threat can be referred to as *'how'* information, as opposed to *'why'* information specifying why one threatens. This distinction stems from research on action identification (Vallacher & Wegner, 1987) and reflects levels of abstractness at which people mentally represent past and future situations such as memories, speculations or plans (Soderberg, Callahan, Kochersberger, Amit, & Ledgerwood, 2015). A recent study showed that actualizers provided less *'how'* information than bluffers when communicating their threat, whereas the two groups provided a comparable amount of *'why'* information (Geurts, Granhag, Ask, & Vrij, 2016).

It is theorized that the need to be believed is more urgent for bluffers than for actualizers. Actualizers have a follow-up plan in

case the threat does not pay off (they can implement the threat), whereas bluffers have not. Bluffers thus depend entirely on the target's conviction and willingness to meet their demands. This could make bluffers more sensitive to the response of the target, for example when the target raises suspicion towards them.

In the present study, we examined verbal threat strategies by interviewing participants who express a threat that they intend to actualize (*actualizers*) or not (*bluffers*). Participants were given the opportunity to express a threat over the phone (*free-statement phase*), and were then asked questions about the expressed threat (*specific-questions phase*). These questions were meant to induce different levels of perceived interviewer suspicion. Half of the participants were asked questions/prompts suggesting that the interviewer wanted to assess the veracity of the threat (*high-suspicion protocol*), whereas the other half were asked questions/prompts suggesting that the interviewer wanted to better understand what the threatener was saying (*low-suspicion protocol*).

Both bluffers and actualizers are theorized to be forthcoming when making a threat and we had no reason to expect differences in their statements during the free-statement phase. However, we propose that it is relatively more important for bluffers to convince their target, which will make bluffers comparatively more sensitive to questioning. We therefore predicted an interaction effect between interview phase and threat veracity on the amount of information provided, with bluffers becoming relatively more forthcoming than actualizers when being subjected to specific questions (Hypothesis 1). Furthermore, we propose that bluffers are more attentive to suspicion against them. Therefore, we predicted that differences between bluffers and actualizers become larger when they are faced with the high-suspicion protocol compared to the low-suspicion protocol, with bluffers perceiving greater increases in suspicion towards them (Hypothesis 2) and with bluffers providing greater increases of information from the free-statement phase to the specific-questions phase (Hypothesis 3). Furthermore, we theorize that actualizers experience a need to secure a successful implementation of the threat. As revealing implementation details might increase the risk of getting caught, we predicted that actualizers are more reluctant than bluffers to share implementation aspects of the threat (i.e. 'how' information; Hypothesis 4). Finally, we sought to explore to what extent participants changed their threat strategies during the interview and, if so, why.

Method

Participants and Design

A total of 195 participants, mainly undergraduate students from a Swedish university, took part in the study (134 women, 46 men, 15 missing; $M_{age} = 26.60$ years, $SD = 7.38$ years) in which they made a threat via a phone call. They participated on a voluntary basis and received a movie ticket worth approximately €12 in return. Sixteen participants did not make the call because they (a) felt uncomfortable doing so ($n = 14$), (b) had participated in a similar study before ($n = 1$), or (c) due to a technical failure ($n = 1$). Their data were excluded from further analyses. Hence, a sample of 179 participants remained

(130 women, 46 men, 3 other; $M_{age} = 26.60$ years, $SD = 7.35$ years). Participants were randomly assigned as bluffers ($n = 90$) or actualizers ($n = 89$). Furthermore, a random half of the bluffers and actualizers were assigned to be questioned with the high-suspicion protocol ($n = 91$), and the other half were assigned to be questioned with the low-suspicion protocol ($n = 88$).

Procedure

The procedure largely resembled the threat paradigm developed by Geurts and colleagues (2016). Participants were presented with a case that reflected a moral conflict between a fictive Non-Governmental Organization (NGO) named Aware and a fictive clothing company named Vera. Participants read how Aware was dedicated to improving working conditions in low-wage countries and how Vera was known as being socially engaged in the local communities in the countries where Vera outsourced their production. Vera had recently released a commercial in which they drew attention to violence against women. Meanwhile, Aware got hold of video recordings showing how Vera exploited women in factories in Cambodia. Aware considered it hypocritical that Vera raised public awareness about violence against women while simultaneously exploiting them for their own profit. Aware therefore decided to take action against Vera. Participants were instructed to imagine being part of Aware and to represent Aware in this action.

All participants were instructed to call a representative of Vera. They were instructed to threaten to leak the video recordings containing evidence of Vera's malpractice to the media, unless the company withdrew their commercial from television. Participants were either instructed to bluff when making this claim and thus not truly leak the recordings (bluffers), or to do as they claimed and leak the recordings right after the call (actualizers). All participants were given 15 minutes to prepare for their task(s) and all had access to the same background materials (e.g., information about Aware, working conditions in Cambodia, route to the delivery location for the recordings).

Next, the participants phoned the representative of Vera. The recipient of the call was a confederate who responded to the threats according to structured interview protocols, displayed in Table 1. Each participant was initially invited to speak freely (free-statement phase) and was then questioned about the threat he or she made (specific-questions phase). Half of the participants were asked high-suspicion questions/prompts, suggesting that the interviewer aimed to assess the truthfulness of the threat (high-suspicion protocol; e.g., "How do I know that what you are saying is true?"). The other half were asked low-suspicion questions/prompts, suggesting that the interviewer aimed to better understand the threat (low-suspicion protocol; e.g., "To make sure that I get you right, I need to know more").

After the call, the experimenter informed the participants that the Vera representative thought they were bluffing and therefore decided to ignore the threat. They were then instructed to proceed with their task according to the instructions. Bluffers were supposed to do nothing, whereas actualizers were supposed to provide their media contact with a USB stick containing

Table 1
Interview Protocols That Were Used to Answer the Participants' Threat Calls

Free-statement phase	
Hello, my name is Caroline. I'm the head of public relations at Vera's and I expected your call. You initiated this conversation, so please go ahead.	
Specific-questions phase	
Low-suspicion protocol	High-suspicion protocol
The reason that I take this call is because it is my responsibility <i>to understand you correctly</i> . Therefore I would like to ask you to provide me more information.	The reason that I take this call is because it is my responsibility <i>to find out whether or not you are telling the truth</i> . Therefore I would like to ask you to provide me more information.
Thank you. But this is not yet enough for me <i>to draw the entire picture. To complete my task and make sure that I get you right, I need to know more.</i>	Thank you. But this is not yet enough for me <i>to make a proper judgement. How do I know that what you are saying is true?</i>
Before we finish this conversation, is there anything else that <i>I should know of?</i>	Before we finish this conversation, is there anything else that <i>could further convince me?</i>

Note: Italics indicate words that differed between the interview protocols.

the video recordings. They were intercepted immediately after starting the implementation (e.g., walked towards the door).

Each participant was then asked to answer closed and open-ended questions about the strategies they had used in their communication with Vera. They were asked whether or not they had used any particular strategy (if so, to describe this strategy) and whether they had changed their strategy during the call (if so, to explain why).

Next, each participant completed the perceived suspicion scale by rating three items; "Vera believed me", "Vera trusted me", and "Vera was suspicious of me" (Buller, Strzyzewski, & Comstock, 1991; $\alpha = .68$). To compute an overall measure of perceived suspicion, the average score on the three items was calculated after reversing two of the three items (belief, trust) so that a higher score on the items reflected a higher level of perceived suspicion. Each participant further rated nine statements related to their involvement in the case (e.g., "It is important that action is taken against Vera"; $\alpha = .74$), their belief in the authenticity of the case, how difficult they had found the instructions and their task, how nervous they had been for their task, how sufficient the time for preparation had been, and how willing they had been to give Vera information. All scales ranged from 1 (*not at all*) to 7 (*very much*). Participants were then thoroughly debriefed, thanked for their participation, and handed the movie ticket.

Codings

Provided Information. Two trained coders coded the transcribed calls. Each transcript was coded for (a) the total amount information revealed, which was further broken down into the amount of (b) 'why' and (c) 'how' information,

reflecting Vallacher and Wegner's (1987) distinction between 'why' aspects of an action (why to threaten) and 'how' aspects of an action (how to enact the threat). An existing coding scheme was used, developed for a previous study (Geurts et al., 2016). The scheme included 76 pieces of information in the background materials to which the participants had access to while preparing the call. Of this total, 44 pieces were classified as 'why' information, and 32 pieces were classified as 'how' information. For instance, explanations about the poor conditions in Cambodia, the malpractice of Vera, or the vision of Aweare were classified as 'why' information. Moreover, details such as the delivery location or the name of the media contact were classified as 'how' information. Each transcript was coded for new pieces of information. A piece of information was considered new when it was mentioned for the first time by the participant. Repetitions were thus not taken into account. Two coders coded 20% of the transcripts, resulting in agreement on 92% of the decisions made (Cohen's $\kappa = .77$). One of the coders completed the remaining 80% of the transcripts. The coders were blind to the condition of the participants and to the hypotheses of the study.

Reported strategies. Two coders coded the answers provided for the strategy question (i.e., "Describe the strategy you used during your communication with Vera"). Reported strategies were divided into two categories, mirroring the previously described 'how' versus 'why' division. Strategies focused on the implementation of the threat were classified as 'how' strategies (e.g., "My strategy was to convince Vera that I really had the material, and that giving it to my contact would be problematic for them"). Strategies focused on motivating the threat were classified as 'why' strategies (e.g., "I tried to make Vera realize that their business operation is hypocrite"). When participants reported both type of strategies, only the main strategy was coded (e.g., the following statement was coded as a 'how' strategy, "My strategy was to show my power by pointing at the USB stick in my hand. I also tried to be informative"). When both types of strategies were equally prevalent, it was coded as "both" (e.g., "I tried to make clear that their vision went against the actual working conditions. I pointed out that I had proof and was ready to reveal the proof to the public"). Strategies that fitted neither one of the two categories were classified as "other". After the coders coded 20% of the answers and reached an inter-rater agreement of 86% (Cohen's $\kappa = .70$), one coder proceeded with the remaining material. Again, the coders were unaware of the conditions and hypotheses.

Change of Strategies. The open-ended question on strategy change (i.e., "Explain why you changed strategy during the communication with Vera") was included for exploratory purposes. Hence, a data-driven scheme was used to code the participants' answers, meaning that one individual, blind to the conditions, used the answers to identify broader categories in the data. Four reasons for strategy change were identified: (1) the participant did not get the response that they had wanted/expected, (2) the participant was asked to provide more information, (3) the participant was asked to prove their point, and/or (4) the conversation was coming to an end. It was possible for participants to report more than one reason. Reasons that fitted neither one of the four mentioned categories were classified as 'other'. Two individuals

coded 20% of the material. After calculating the interrater agreement (93%, Cohen's $\kappa = .73$), one coder completed the remaining material.

To reiterate, the experimental design involved suspects making a threatening phone call to a company. The threat was about leaking a video containing evidence of malpractice. The phone call included two sections; a free report section initiated by the threatener, followed by a series of prompts initiated by the company. Manipulations were made with respect to the instructions to the threateners ("bluff about the threat" vs. "actualize the threat") and with respect to the level of suspicion raised by the company in the prompts (high vs. low). The dependent variables were (i) the amount of ('how' and 'why') information provided in each section of the threat statement, (ii) the self-reported strategies used to present the case, and (iii) the self-reported reasons for strategy change.

Results

Manipulation Checks

The descriptive statistics of the participants' self-ratings are displayed in Table 2. The table reveals that participants assessed the case as authentic, rated high involvement with Aweare's case against Vera, understood the instructions, and reported that they had sufficient time to prepare their tasks. Yet, participants found their tasks demanding and were nervous about completing them. This was true for both making the threat call and for delivering the USB stick (the latter was rated by actualizers only). Independent *t*-tests showed that none of these measures differed significantly between actualizers and bluffers, all *t*s (177) < 1.81, *p*s > .07.

Actualizers and bluffers were supposed to have different intentions with regard to delivering the USB stick. Actualizers were supposed to deliver the stick immediately after making the threat call, whereas bluffers were not. To check if all participants acted accordingly, the experimenter waited for the participants to initiate or not initiate the first move towards delivery (e.g., walk towards the door). All actualizers started the implementation, whereas none of the bluffers did. Hence, the manipulation of intent was considered successful.

Table 2
Mean Values (and Standard Deviations) of Bluffers' and Actualizers' Involvement with the Case, Experienced Difficulty to Comply with the Instructions, and Nervousness about Performing the Tasks

Rating	Bluffer	Actualizer
Involvement with case	5.52 (0.77)	5.66 (0.77)
Belief that case rested on authentic facts	5.69 (1.36)	5.94 (1.04)
Understanding of instructions	5.92 (1.03)	5.89 (1.12)
Sufficiency of preparation time	4.81 (1.79)	4.31 (1.80)
Difficulty making call	4.82 (1.51)	4.67 (1.75)
Difficulty preparing delivery	N/A	2.86 (1.62)
Nervousness about making call	5.13 (1.65)	5.28 (1.69)
Nervousness about delivering	N/A	2.94 (1.87)

Note: There were no significant differences between bluffers and actualizers on the reported ratings (*p* > .05). All ratings were made on 7-point Likert scales (1 = not at all, 7 = very much).

Perceived Suspicion

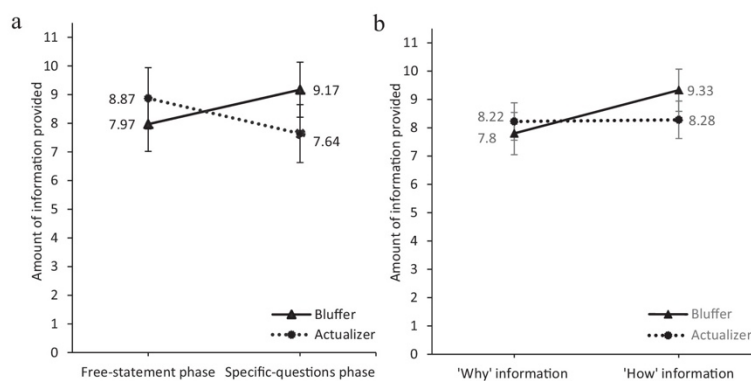
A 2 (threat: bluff vs. actualize) \times 2 (protocol: high suspicion vs. low suspicion) between-subjects ANOVA on the level of perceived suspicion, revealed a main effect of protocol, $F(1, 175) = 11.53$, $p = .001$, $\eta_p^2 = .06$. The participants who were questioned with the high-suspicion protocol reported to have experienced more suspicion directed towards them ($M = 5.44$, $SD = 1.00$) than the participants questioned with the low-suspicion protocol ($M = 4.93$, $SD = 1.03$), which supports the effectiveness of the protocols. Note that both protocols induced suspicion awareness, and the low-suspicion protocol thus refers to *lower* (rather than low) suspicion induction compared to the high-suspicion protocol. Furthermore, there was no main effect of threat, $F(1, 175) = 2.90$, $p = .090$, $\eta_p^2 = .02$. In contrast to Hypotheses 2, no significant interaction was found between threat and protocol, $F(1, 175) = 0.83$, $p = .364$, $\eta_p^2 = .01$. Bluffers and actualizers experienced similar levels of suspicion in the low-suspicion protocol ($M_{\text{bluff}} = 4.73$, $SD = 1.00$; $M_{\text{actualize}} = 5.13$, $SD = 1.03$), as well as in the high-suspicion protocol ($M_{\text{bluff}} = 5.38$, $SD = 1.07$; $M_{\text{actualize}} = 5.50$, $SD = 0.92$). Thus, the highly suspicious questions affected bluffers' and actualizers' perceived suspicion to the same extent.

Provided Information

It was found that all participants were fairly forthcoming in the free-statement phase. About half of the total amount of information given by bluffers and actualizers was provided during the free-statement phase (bluffers 47%, actualizers 54%). This finding was further supported by the participants' self-rated willingness to share information, showing that both bluffers ($M = 5.02$, $SD = 1.57$) and actualizers ($M = 5.40$, $SD = 1.39$) were rather willing to share information, $t(177) = -1.72$, $p = .086$, $d = .26$, 95% CI [-.551, .038]. The willingness rating was significantly related to the actual amount of information provided in the interview, $r = .20$, 95% CI [.059, .353], $p = .008$.

To test the hypotheses with regard to information provision (H1, H3, and H4), three separate ANOVA's were conducted. The descriptive statistics of all three analyses are displayed in Table 3. First, a 2 (threat: bluff vs. actualize) \times 2 (phase: free-statement vs. specific-questions) mixed ANOVA was performed on the total amount of details provided in the statements, with Threat as the between-subjects factor, and Phase as the within-subjects factor. The analysis revealed no main effects of Threat, $F(1, 177) = 0.66$, $p = .419$, $\eta_p^2 = .00$, or Phase, $F(1, 177) = 0.00$, $p = .983$, $\eta_p^2 = .00$. However, there was a significant Threat \times Phase interaction effect, $F(1, 177) = 4.19$, $p = .042$, $\eta_p^2 = .02$. Tests of simple effects provided support for Hypothesis 1. As can be seen in Figure 1a, bluffers provided more information in the specific-question phase than actualizers did, $F(1, 177) = 4.74$, $p = .031$, $\eta_p^2 = .03$, whereas no such difference was found for the free-statement phase, $F(1, 177) = 1.58$, $p = .211$, $\eta_p^2 = .01$.

Second, to test the influence of suspicion, a 2 (threat: bluff vs. actualize) \times 2 (protocol: high suspicion vs. low suspicion) between-subjects ANOVA was conducted on the information



Note. Error bars denote 95% confidence intervals.

Figure 1. (a) Total amount of information provided by bluffers and actualizers in the free-statement phase and in the specific-questions phase. (b) Amount of 'why' and 'how' information provided by bluffers and actualizers.

provided in the specific-questions phase. Already reported, bluffers provided more information in the specific-question phase compared to actualizers, hence a significant main effect of Threat was found, $F(1, 175) = 4.89, p = .028, \eta_p^2 = .03$. There was no main effect for Protocol, $F(1, 175) = 4.89, p = .028, \eta_p^2 = .03$. Importantly, no support was found for Hypothesis 3. The mean values even suggest an opposite trend. That is, bluffers provided more information than actualizers when questioned under low suspicion (rather than under high suspicion), but this Threat \times Protocol interaction was not found statistically significant, $F(1, 175) = 2.85, p = .093, \eta_p^2 = .02$.

Third, a 2 (threat: bluff vs. actualize) \times 2 (information: how vs. why) mixed ANOVA was performed to examine the type of information provided by bluffers and actualizers. No main effect of Threat was found, $F(1, 177) = 0.66, p = .419, \eta_p^2 = .00$.

Table 3
Mean Values (and Standard Deviations) for the Amount of Information that Bluffers and Actualizer Provided in their Threat Statements by Phase, Protocol, and Information

Threat	Free-statement phase	Specific-questions phase
	<i>M (SD)</i>	<i>M (SD)</i>
Bluffer	7.97 (4.52)	9.17 (4.60)
Actualizer	8.87 (5.04)	7.64 (4.78)
Threat	Low-suspicion protocol	High-suspicion protocol
	<i>M (SD)</i>	<i>M (SD)</i>
Bluffer	9.84 (4.78)	8.52 (4.37)
Actualizer	7.11 (4.93)	8.16 (4.62)
Threat	'How' information	'Why' information
	<i>M (SD)</i>	<i>M (SD)</i>
Bluffer	9.33 (3.56)	7.80 (3.53)
Actualizer	8.28 (3.33)	8.22 (3.13)

However, the analysis revealed a main effect of Information $F(1, 177) = 5.86, p = .017, \eta_p^2 = .03$, showing that participants revealed more 'how' than 'why' information. There was a significant Threat \times Information interaction, $F(1, 177) = 5.06, p = .026, \eta_p^2 = .03$. In support of Hypothesis 4, simple effect tests revealed that bluffers provided significantly more 'how' details throughout their statement than actualizers did, $F(1, 177) = 4.14, p = .043, \eta_p^2 = .02$, whereas no significant difference between the groups was found for the amount of 'why' details provided, $F(1, 177) = 0.73, p = .396, \eta_p^2 = .00$. This effect is displayed in Figure 1b.

Strategies

Nearly all participants reported to have used some strategy when communicating the threat (94%). Chi-square analyses revealed that bluffers and actualizers reported to have used 'how' and 'why' strategies to an equal extent (see Table 4). Hence, the findings on reported strategies lend no further support to Hypothesis 4.

Out of 164 participants who reported to have had a strategy, 82 (50%) reported to have changed strategy during the conversation. Participants reported to have changed strategy (a) because the response from Vera differed from what they had wanted/expected (42%; e.g., "When I noticed a lack of moral response, I tried to install fear"), (b) because they were asked to provide more information (29%; e.g., "When I suddenly was asked to clarify my point, I tried to explain how they violate human rights"), (c) because they were asked to prove their point (17%; e.g., "When Vera wanted me to show that I was telling the truth, I tried to rethink and express myself differently"), (d) because the end of the conversation was approaching (10%; e.g., "Towards the end, when Vera did not sound convinced, I tried to push more towards the fact that it was in their own interest"), and/or (e) for other reasons (6%; e.g., "I lost what I was going to say and strayed away from my strategy"). Seven

Table 4
Reported Strategies by Bluffers and Actualizers

Strategy	Bluffers	Actualizers	χ^2	p	φ
Why (focus on explaining the threat)	29 (32%)	33 (37%)	0.47	.495	.05
How (focus on implementing the threat)	32 (36%)	31 (35%)	0.01	.919	.01
Both ('how'/'why' to an equal extent)	5 (6%)	9 (10%)	1.29	.256	.08
Other	16 (18%)	13 (15%)	0.33	.565	.04
No strategy	8 (9%)	3 (3%)	2.36	.124	.11

participants (9%) did not report the reason for their change of strategy. Chi-square analyses revealed no significant differences between bluffers and actualizers for the number of strategy changes or for the type of reasons reported ($\chi^2 < 3.84$).

An explorative analysis was conducted to examine the influence of suspicion on the number of strategy changes reported. A chi-square analysis showed that a comparable percentage of participants interviewed under low suspicion (43.4%) and high suspicion (56.8%) made strategy changes, χ^2 (1, $N=164$) = 2.95, $p = .086$, $\varphi = .13$.

In addition, the relation between strategy change and information provision was further explored in a mixed Change (yes vs. no) \times Phase (free-statement vs. specific-questions) ANOVA on the amount of information provided. Note that only the participants who reported to have used a strategy were included in the analysis ($n=164$). The analysis yielded a near-significant Change \times Phase interaction, $F(1, 162) = 3.64$, $p = .058$, $\eta_p^2 = .02$. The trend in the data points out that participants who reported a shift in strategy, increased their information provision from the free-statement phase ($M = 7.96$, $SD = 4.91$) to the specific-question phase ($M = 8.96$, $SD = 4.99$), whereas participants who reported no shift in strategy decreased their information provision from the free-statement phase ($M = 8.93$, $SD = 4.67$) to the specific-question phase ($M = 7.54$, $SD = 4.49$).

At last, the correlation was tested between type of strategies reported (how vs. why) and type of information provided (how vs. why). A positive correlation was found between the reported use of 'why' strategies and the amount of 'why' information provided, $r_{pb} = .338$, $p < .001$. No correlation was found between the reported use of 'how' strategies and the provision of 'how' information, $r_{pb} = .072$, $p = .422$.

Discussion

Major Findings

Our findings suggest that people avail of self-regulative mechanisms when communicating threats. Threatening participants were found to be forthcoming, strategic, and adaptive to the target's response. Both bluffers and actualizers were willing to share information, which fits well with the experience of professionals who report that threateners are typically eager to discuss their case (Van der Meer & Diekhuis, 2013; White, 2013). Furthermore, almost all participants (94%) reported to have used a strategy in their communication with the target. Half of these participants changed their strategy during the communication, thereby adapting to the situation. It is worth noting that threatening participants combined a typical innocent-suspect attitude (*being forthcoming*, e.g., Strömwall et al., 2006) with a

typical guilty-suspect attitude (*being strategic*, e.g., Hartwig et al., 2007). This might be the result of the confounding of guilt and innocence when stating a threat. Bluffers may have no intent to cause harm, but they are guilty of lying about their intentions (i.e., innocent liars). In contrast, actualizers intimidate the target with truthful intentions but they are honest in their claim (i.e., guilty truth-tellers).

It was predicted and found that bluffers provided more information than actualizers when being questioned about the threat, but, in contrast to our prediction, this difference was not affected by the suspicion manipulation. This might be the result of bluffers and actualizers reporting to have experienced similar levels of perceived suspicion. Thus, bluffers were not particularly receptive to suspicion, neither were they more affected by it. The findings contradict previous studies in which lying interviewees (which bluffers can be considered to be) were found to be more aware of the risk for not being believed (Hartwig et al., 2010), more attentive to the interviewer's suspicion (Vrij, Fisher, Mann, & Leal, 2008), and more forthcoming when asked critical questions, compared to truth-telling interviewees (Geurts et al., 2016). Overall, the low-suspicion protocol showed more potential for eliciting differences between bluffers' and actualizers' statements. Research has shown that information-gathering interview styles typically elicit more, and more correct information from mock suspects than accusatorial interview styles do (Meissner, Redlich, Bhatt, & Brandon, 2012; Vrij, Mann, Kristen, & Fisher, 2007). However, information-gathering interviewing has not been found to elicit differences between liars and truth-tellers with regard to statement length (Vrij et al., 2007).

Consistent with our hypothesis, actualizers revealed less information about the implementation of the threat ('how' information) compared to bluffers. This finding might seem counter-intuitive at first as it could be reasoned that the more implementation details specified in a threat statement, the higher the risk is for actual implementation. Previous research has supported this logic. It has been found that people tend to give more concrete accounts when describing near future events (Wakslak, Trope, Liberman, & Alony, 2006) and true intentions (Mac Giolla, Granhag, & Vrij, 2015). However, the opposite was found in a recent study on threats, showing that actualizers provided less 'how' details than did bluffers (Geurts et al., 2016). It was suggested that actualizers might have had many 'how' details in mind, but decided to keep this information to themselves to prevent the risk of getting caught.

The current finding lends further support to this idea, although caution is warranted for a number of reasons. First, the study did not measure how many 'how' or 'why' details the participants kept in mind without telling. It is only known

how many details they had access to and how many details they revealed. Second, risk perception was not measured in this study. That is, participants did not rate how risky they thought it was to reveal certain details. Third, the difference in provided 'how' information was not reflected in the self-reported strategies of bluffers and actualizers. Strategies meant to explain the motives behind the threat (i.e., 'why' strategies) and strategies meant to prove the capacity to implement the threat (i.e., 'how' strategies) were reported as often by bluffers as by actualizers. Thus, the current study provides partial support for the hypothesis that actualizers are more reluctant than bluffers to share implementation details. Looking at the threat statements, actualizers indeed placed less emphasis on implementation details, but their self-reported strategies did not provide evidence for that this was the result of a conscious decision.

Limitations

Although the predicted differences between bluffers and actualizers were partly confirmed, the current study did not provide a clear insight into the processes explaining these differences. Some possible mediators were not explicitly measured (e.g., that actualizers find implementation details risky to reveal; that bluffers are more concerned about their credibility), and others could not be properly established (e.g., that bluffers perceive more suspicion directed towards them; that actualizers intentionally conceal 'how' details). Future research should examine such factors in a more thorough manner. Making participants aware of the dilemma they face (e.g., "Note that revealing some details might increase the risk of getting caught") might further enhance differences between bluffers and actualizers.

Furthermore, two more general shortcomings should be addressed. The student sample used may speak against the external validity of the study. In terms of wellbeing, it can be argued that the average student differs from the average person who poses a threat of violence. Moreover, the issues that are typically at stake in real-life threat cases (e.g., money, housing, marriage, custody) are difficult (if not impossible) to mirror in the lab. Hence, the participants plausibly felt less personally involved compared to actual threateners.

The magnitudes of the differences found between bluffers and actualizers were small to moderate. Small differences may be valuable on a theoretical level, as these could tell something about underlying mechanisms that are at play, but on an operational level it is unlikely that small behavioral differences can be detected by professionals who interact with subjects of concern. Hence, the current findings cannot (at this early stage) serve as cues to detect bluffs or actual danger. With that said, it could be argued that the effects found in the lab may be larger in real life. Research has shown that self-regulation becomes particularly present in aversive situations in which the course and the outcome of an event is uncertain (Fiske & Taylor, 2008).

Contribution to the Field

The current findings support the proposition that threatening is a deliberate act, for which people prepare themselves

strategically, regardless of whether or not they intend to enact the threat. The idea that threateners pursue their own agenda during interviews—and may be unwilling to reveal all they know—has been raised as a reason to focus on other sources of information (Meloy et al., 2013). However, we argue that threat assessment interviews may be an important information-gathering tool as long as the interviewer understands, and adapts to, the counter-interview strategies used by the interviewee. This study aimed to contribute to such understanding. Knowing what interview dynamics can be expected may not only improve the quality of threat assessment interviews, it may also lower the threshold for professionals to interact directly with subjects of concern.

Conflict of Interest Statement

The authors declare that they have no conflict of interest.

Author Contributions

The first three authors were equally involved in the conceptualization and design of the study. The first author had the main responsibilities for data collection, data analysis, and writing the manuscript. All authors were involved in subsequent revisions of the manuscript.

Acknowledgements

This research was funded by the Erasmus Mundus Joint Doctoral program in Legal Psychology. We would like to thank Mandy Sundborg and Therese Wallstedt for their help with data collection.

References

- Buller, D. B., Strzyzewski, K. D., & Comstock, J. (1991). *Interpersonal deception: I. Deceivers' reactions to receivers' suspicions and probing*. *Communications Monographs*, 58, 1–24.
- Fiske, S. T., & Taylor, S. E. (2008). *Social cognition: From brains to culture*.
- Geurts, R., Granhag, P. A., Ask, K., & Vrij, A. (2016). Taking threats to the lab: Introducing an experimental paradigm for studying verbal threats. *Journal of Threat Assessment and Management*, 53–64.
- Granhag, P. A., Clemens, F., & Strömwall, L. A. (2009). The usual and the unusual suspects: Level of suspicion and counter-interrogation tactics. *Journal of Investigative Psychology and Offender Profiling*, 6, 129–137.
- Granhag, P. A., & Hartwig, M. (2008). A new theoretical perspective on deception detection: On the psychology of instrumental mind-reading. *Psychology, Crime & Law*, 14, 189–200.
- Granhag, P. A., & Hartwig, M. (2015). The Strategic Use of Evidence (SUE) technique: A conceptual overview. In P. A. Granhag, A. Vrij, & B. Verschuere (Eds.), *Detecting deception: Current challenges and cognitive approaches* (pp. 231–251). UK: Wiley Blackwell.
- Granhag, P. A., Hartwig, M., Giolla, E. M., & Clemens, F. (2015). Suspects' verbal counter-interrogation strategies. In P. A. Granhag, A. Vrij, & B. Verschuere (Eds.), *Detecting deception: Current challenges and cognitive approaches* (pp. 293–313). UK: Wiley Blackwell.
- Hartwig, M., Granhag, P. A., Strömwall, L. A., & Doering, N. (2010). *Impression and information management: On the strategic*

- self-regulation of innocent and guilty suspects. *The Open Criminology Journal*, 3, 10–16.
- Hartwig, M., Granhag, P. A., & Strömwall, L. A. (2007). Guilty and innocent suspects' strategies during police interrogations. *Psychology, Crime & Law*, 13, 213–227.
- Hines, A., Colwell, K., Hiscock-Anisman, C., Garrett, E., Ansarra, R., & Montalvo, L. (2010). Impression management strategies of deceivers and honest reporters in an investigative interview. *The European Journal of Psychology Applied to Legal Context*, 2, 73–90.
- Luke, T. J., Dawson, E., Hartwig, M., & Granhag, P. A. (2014). How awareness of possible evidence induces forthcoming counter-interrogation strategies. *Applied Cognitive Psychology*, 28, 876–882.
- Mac Giolla, E., Granhag, P. A., & Vrij, A. (2015). Discriminating between true and false intentions. In P. A. Granhag, A. Vrij, & B. Verschuere (Eds.), *Deception detection: Current challenges and cognitive approaches* (pp. 155–173). UK: Wiley Blackwell.
- Meissner, C., Redlich, A., Bhatt, S., & Brandon, S. (2012). Interview and interrogation methods and their effects on investigative outcomes. *Campbell Systematic Reviews*, 8.
- Meloy, J. R., Hart, S. D., & Hoffmann, J. (2013). Threat assessment and threat management. In J. R. Meloy, & J. Hoffmann (Eds.), *International handbook of threat assessment* (pp. 3–17). New York, NY: Oxford University Press.
- Oleszkiewicz, S., Granhag, P. A., & Cancino Montecinos, S. (2014). The Scharff-technique: Eliciting intelligence from human sources. *Law and Human Behavior*, 38, 478–489.
- Soderberg, C. K., Callahan, S. P., Kochersberger, A. O., Amit, E., & Ledgerwood, A. (2015). The effects of psychological distance on abstraction: Two meta-analyses. *Psychological Bulletin*, 141, 525–548.
- Strömwall, L. A., Hartwig, M., & Granhag, P. A. (2006). To act truthfully: Nonverbal behavior and strategies during a police interrogation. *Psychology, Crime & Law*, 12, 207–219.
- Tekin, S., Granhag, P. A., Strömwall, L., Giolla, E. M., Vrij, A., & Hartwig, M. (2015). Interviewing strategically to elicit admissions from guilty suspects. *Law and Human Behavior*, 39, 244–252.
- Vallacher, R. R., & Wegner, D. M. (1987). What do people think they're doing? Action identification and human behavior. *Psychological Review*, 94, 3–15.
- Van der Meer, B. B., & Diekhuis, M. L. (2013). Collecting and assessing information for threat assessment. In J. R. Meloy, & J. Hoffmann (Eds.), *International handbook of threat assessment* (pp. 54–66). New York, NY: Oxford University Press.
- Vrij, A., Fisher, R., Mann, S., & Leal, S. (2008). A cognitive load approach to lie detection. *Journal of Investigative Psychology and Offender Profiling*, 5, 39–43.
- Vrij, A., Mann, S., Kristen, S., & Fisher, R. P. (2007). Cues to deception and ability to detect lies as a function of police interview styles. *Law and Human Behavior*, 31, 499–518.
- Wakslak, C. J., Trope, Y., Liberman, N., & Alony, R. (2006). Seeing the forest when entry is unlikely: Probability and the mental representation of events. *Journal of Experimental Psychology: General*, 135, 641–653.
- White, S. G. (2013). Workplace targeted violence. In J. R. Meloy, & J. Hoffmann (Eds.), *International handbook of threat assessment* (pp. 83–106). New York, NY: Oxford University Press.

Received 1 October 2016;
 accepted 6 October 2016
 Available online 29 November 2016

Appendix G: Manuscript Study III

Interviewing to Manage Threats: Exploring the Effects of Interview Style on Information Gain and
Threateners' Counter-Interview Strategies

Renate Geurts*

University of Gothenburg, Sweden

University of Portsmouth, England

Karl Ask

University of Gothenburg, Sweden

Pär Anders Granhag

University of Gothenburg, Sweden

Norwegian Police University College, Norway

Aldert Vrij

University of Portsmouth, England

*Corresponding author

Department of Psychology, University of Gothenburg

P.O. Box 500, 405 30 Gothenburg, Sweden

E-mail: renate.geurts@psy.gu.se

Phone: +46317864283

This work was supported by the Erasmus Mundus Joint Doctoral program in Legal Psychology (EMJD-LP) under Framework Partnership Agreement (FPA) 2013-0036 and Specific Grant Agreement (SGA) 2014-0678.

Abstract

There is consensus about the importance to engage with, and if possible interview, individuals who threaten to cause harm. However, there exist little research on how to conduct such interviews. This paper contributes with an experimental approach on threat management interviewing. We explored what types of counter-interview strategies threateners employ, and we tested the efficacy of two common interview styles (direct interviewing vs. rapport-based interviewing). Participants ($N = 120$) were interviewed about a threat they had made, and reported what strategies they had used during the interview. No differences were found between protocols for threat management outcomes (i.e. information gain, use of counter-interview strategies, and willingness to discuss or enact the threat). However, the study showed how threateners stroke a deliberate balance between proving their stand and disguising implementation details. Critically, individuals with more serious intentions to enact the threat were more inclined to hide information from the interviewer. We argue that it is vital for threat management interviewing to i) understand what behaviors can be expected from the interviewee, and ii) learn about interview methods that can steer these behaviors towards information gain (which is beneficial to threat assessment) and towards de-escalation (which is the purpose of threat management).

Keywords: threat management, threat assessment, investigative interviewing, counter-interview strategy

Interviewing to Manage Threats: Exploring the Effects of Interview Style on Information Gain and Threateners' Counter-Interview Strategies

Most threats of violence will never be enacted (Warren, Mullen, & McEwan, 2014), but the threats that are enacted often come with high costs (e.g. human lives, financial damage). This warrants a careful assessment of each individual threat. The goal for threat management is not to predict who will or will not commit harm, but rather to triage among a number of worrisome cases (James & Farnham, 2016; Gill, 2015). In this triage process, threat managers typically express an overall level of concern (low, medium, high), and this level informs what interventions are needed to mitigate the risks for the individual case (Meloy, Hoffmann, Guldinann, & James, 2012). To reach such an assessment, information is needed about the subject of concern. For instance, threat managers must find out about the subject's motivation, intentions, mental health, and his or her capability to cause harm (Vossekuil, Fein, & Berglund, 2015). In part this information can be extracted from databases (e.g. police, social services), but the most direct source of information is the subject him or herself. The importance of interviewing subjects of concern has been widely acknowledged in the literature on threat assessment and management (Calhoun & Weston, 2015; Fein & Vossekuil, 1998; van der Meer & Diekhuis, 2014). It is therefore surprising that there is hardly any research on how to conduct such interviews. The few publications that do exist on the theme draw largely on the authors' professional experiences (e.g. Meloy & Mohandie, 2014; van der Meer & Diekhuis, 2014). This paper contributes with an experimental approach to threat management interviewing. We present a study on how to elicit valuable information from people who pose a threat—in this paper referred to as *threateners*. Specifically, the current study examines the efficacy of two general interview styles applied in law enforcement and intelligence contexts: *direct interviewing* and *rapport-based interviewing* (Alison, et al., 2014; Justice, Bhatt, Brandon, & Kleinman, 2010).

Counter-Interview Strategies

It could be argued that successful interviewing starts with understanding the interviewee's perspective (Granhag & Hartwig, 2008). Perspective taking allows the interviewer to adapt to the strategies and the needs of the interviewee (Galinsky, Maddux, Gilin, & White, 2008). Many interviewees in legal contexts are semi-cooperative, meaning that the interviewee benefits from

revealing some, but not all, information they hold. For instance, guilty suspects want to be perceived as truthful without disclosing incriminating details (Hartwig, Granhag, Strömwall, & Doering, 2010; Tekin et al., 2015). Moreover, sources who hold information about an upcoming crime may want to warn the police without revealing that their friends are involved (Dalgaard-Nielsen, 2013; Granhag, Kleinman, & Oleszkiewicz, 2016). Threateners arguably face a similar dilemma; they need to make sure that they are taken seriously without being too specific about their intentions (Geurts, Ask, Granhag, & Vrij, 2016). Many interviewees must thus manage the information they reveal and the impression they make (Hartwig et al., 2010). Such management efforts are referred to as *counter-interview strategies* (Granhag, Clemens, & Strömwall, 2009).

Interview techniques that build on the counter-interview strategies of interviewees have proven to be effective in suspect and source interviewing. One such technique is to withhold evidence from the suspect, so that guilty suspects (who wish to conceal incriminating details) produce more inconsistencies in their statements compared to innocent suspects (who wish to reveal what they know). This technique is referred to as the Strategic Use of Evidence (SUE) technique (Granhag & Hartwig, 2015). Another way to anticipate the interviewees' concern of revealing too much information is by creating the illusion that the information they hold is already known by the interviewer (Toliver, 1997). The 'illusion of knowing it all' is intended to elicit new information from the interviewee, while letting them believe they contributed with little or nothing. Recent empirical work has provided support for the efficacy of this tactic (Granhag et al., 2016; Oleszkiewicz, 2016; Oleszkiewicz, Granhag, & Kleinman, 2017).

In order to develop such techniques for threat management purposes, we must first understand what counter-interview strategies threateners employ. A recent study on this topic showed that threateners were forthcoming, yet strategic (Geurts et al., 2016). When interviewed about the threat they had made, threateners were willing to share information but presented their case deliberately (e.g. 'I tried to show I was serious by pointing out that [...]'). This finding implies that individuals who pose a threat—just like suspects and sources—use self-regulative mechanisms during interviews. The present study advances this line of work by exploring what *type* of counter-interview strategies threateners employ.

Rapport-Based Interviewing

The purpose of investigative interviewing is to obtain a reliable and complete account (Evans, Meissner, Brandon, Russano, & Kleinman, 2010). This purpose can be achieved by asking open-ended questions in a business-like manner, so-called direct interviewing (Justice, et al., 2010). Direct interviewing is a common and straightforward interview style but it leaves little room for building rapport, which is considered important for gathering information (Milne, Shaw, & Bull, 2007; Meissner et al., 2014). A clear-cut definition of rapport is difficult to provide, but rapport-based interviewing is often explained as a friendly interview style that is characterised by acceptance, empathy, and respect for the interviewee's autonomy (Saywitz, Larson, Hobbs, & Wells, 2015; Alison, et al., 2014).

A recent literature review on effective interviewing concludes that the best information gatherers are those who can establish and maintain rapport throughout the interview (Bull, 2013). A meta-analysis provides support for this conclusion, demonstrating that information-gathering methods in which rapport is established are more successful in eliciting true confessions (while reducing the likelihood of false confessions), compared to accusatorial questioning methods (Meissner et al., 2014). In addition, rapport-based interviewing has been found to increase the amount of useful information obtained from suspects (Alison, Alison, Noone, Elntib, & Christiansen, 2013), and to reduce the suspects' use of counter-interview strategies (Alison, et al., 2014). These findings fit well with field research showing that offenders report to be more willing to provide a truthful account in response to humane, honest, non-dominant, and respectful interviewing (O Connor & Carson, 2005; Kebbell, Hurren, & Mazerolle, 2006).

Direct interviewing as well as rapport-based interviewing are information-gathering methods (as opposed to accusatorial or confession-oriented methods) that are grounded in psychological theory and research on memory and communication (Hartwig, Luke, & Skerker, 2016). It is here presumed that methods that exploit basic principles of human dynamics are applicable to a wide variety of interview settings, including threat management interviewing.

The Present Study

The first objective of this study was to explore the counter-interview strategies of persons who pose a threat. We argue that learning about interviewees' counter-interview strategies is a necessary starting point for developing interview techniques for threat management. The second objective was to test the comparative efficacy of direct interviewing and rapport-based interviewing. Based on the

findings discussed above that interviewees are more cooperative and willing to be truthful in information-gathering interviews, we predicted that participants interviewed with a rapport-based interview protocol would use fewer counter-interview strategies (Hypothesis 1), provide more information (Hypothesis 2), display a lower willingness to enact the threat (Hypothesis 3), and display a higher willingness to interact (meet) with the conflicting party again (Hypothesis 4), compared to participants interviewed with a direct interview protocol.

Method

Participants and Design

One hundred and twenty students at the University of Gothenburg (33 men, 83 women, 4 other, $M_{age} = 27.38$ years, $SD = 8.83$ years) participated in the experiment on a voluntary basis. Participation took approximately 40 minutes and participants were compensated with 100 SEK (approx. 11 USD). Participants were randomly assigned to one of two interview conditions: direct interviewing ($n = 60$) or rapport-based interviewing ($n = 60$).

Procedure

Participants were recruited for what was advertised as a study on ‘career challenges’. Upon arrival, they read a fictitious case about a work conflict between a consultancy company and a former employee. The case file revealed how the company had allegedly tricked recent graduates into unpaid internships by promising them a permanent position. After the internship, however, their contract was ended and the company had profited from free labor. A duped employee wrote a letter to the company in which s/he threatened to press charges against this malpractice, unless the company would financially compensate her/him for the work carried out. Participants were asked to imagine being this employee. See Appendix A for the full background story and the instructions to the participants.

First, participants were asked to list up to five reasons for why they would press charges at this point in time, as well as reasons for why they would *not* press charges at this point in time. This task was meant to stimulate the participants to think carefully about the case before they rated four items about their *willingness to enact the threat* (i.e. to press charges). Participants rated the extent to which (i) they believed they could win the case in a court of law, (ii) they thought the case was worth pursuing, even if it would be rather expensive, (iii) they thought the case was worth pursuing even if it would take

time, and (iv) they were likely to press charges (1 = *not at all*, 9 = *very much*; $\alpha = .85$). The procedure was repeated for the participants' *willingness to interact* with the company about their case; participants were first asked to list reasons for and against interacting with them at this point in time, and then rated the extent to which (i) they would be willing to communicate with the company if the company would contact them about their case, (ii) they would seek contact with the company to provide the company with information about their case, and (iii) they would seek contact with the company to gather information about their case (1 = *not at all*, 9 = *very much*; $\alpha = .64$).

Next, participants were informed that an employee of the internal security unit from the company would discuss the case with them. Participants were then given 10 minutes to prepare themselves for this meeting and they received additional information about their case (e.g. an overview of the hours they had worked for the company, the contact details of a counsellor). Participants were allowed to make notes and to bring those with them to the meeting. Furthermore, participants were told to keep in mind that 'If you tell too much, the company might take advantage of the information you provide. If you tell too little, the company might not take you seriously'. This was supposed to reflect the information-management dilemma that interviewees in the legal arena typically face (Hartwig et al., 2010; Granhag et al., 2016).

Immediately after the preparation phase, participants were brought to the meeting room. The role of the interviewer was played by one of two confederates (man and woman) who were blind to the hypotheses of the study. The interviewers conducted an equal number of interviews across conditions. All participants received the same 11 questions/prompts. The questions tapped into topics that are considered to be relevant in threat management (e.g. motivation, intentions, capacity; Vossekuil et al., 2015). Half of the participants were approached with a *direct interview protocol*, meaning that the questions/prompts were asked straightforwardly. The other half were approached with a *rappport-based interview protocol*, meaning that the questions/prompts were phrased in a rapport-promoting manner. The interview protocols are displayed in Appendix B.

After the interview, participants rated the same seven items as they had rated before the interview, about their willingness to enact the threat at this point in time (four items, $\alpha = .89$), and about their willingness to interact with the company in the future (three items, $\alpha = .73$). In addition, the

participants were asked to report if they had used a particular strategy when interacting with the interviewer (and if so, to describe this strategy). Finally, participants reported their age, gender, and current occupation.

Protocol Pretesting

The interview protocols were pretested in a separate study. A total of 141 participants (80 men, 61 women) judged to what extent the interview protocols were rapport-promoting. Participants were recruited from Amazon's Mechanical Turk and they were compensated 0.50 USD. Participants were randomly assigned to one of two interview protocols; the direct interview protocol ($n = 73$) or the rapport-based interview protocol ($n = 68$). First, participants read the fictitious case about the work conflict between the consultancy company and the former employee (see Appendix A) so that they would understand the context of the interview questions. Next, they listened to the interview questions as if they were the interviewee. Finally, participants rated 13 items reflecting elements of rapport (e.g. 'The interviewer understands the difficult situation that I am in', see for all items Appendix C). The items were rated on a 7-point Likert scale (1 = *strongly disagree*, 7 = *strongly agree*; $\alpha = .83$).

In support of the design, participants exposed to the rapport-based interview protocol reported significantly higher ratings of rapport ($M = 4.05$, $SD = 0.79$) than participants exposed to the direct interview protocol ($M = 3.55$, $SD = 0.96$), $t(139) = 3.43$, $p < .001$, $d = 0.58$, 95% CI [0.24, 0.91].

Coding

Strategy use. The strategies that the participants reported to have used were divided into six categories; *prove capability*, *explain*, *conceal*, *self-presentation*, *negotiate*, and *other*. Two categories, *conceal* and *self-presentation*, were drawn from previous research on counter-interview strategies of suspects (Hartwig et al., 2010) and two categories, *prove capability* and *explain*, were drawn from previous research on counter-interview strategies of threateners (Geurts et al., 2016). The category *negotiate* was added because of the business-like nature of the case (i.e. work conflict, financial request). Strategies that did not fit any of these five categories were coded as *other*. The participants could report more than one strategy. Two coders, both blind to the hypotheses of the study, categorised the strategies. Based on 20% of the material, an interrater agreement of 87% was established (Cohen's $\kappa = .65$). After settling the disagreements, one coder coded the remaining material.

Information provision. All interviews were transcribed and coded for the amount and type of information disclosed. The background story given to the participants consisted of 45 pieces of information (see Appendix A). These information pieces suited the interview questions (see Appendix B). That is, the participants could use the background information to answer the questions that they were about to receive. For instance, the information piece ‘You kept track of your working hours while working for the company’ could be used to answer the question ‘Why do you think that your case is a strong case?’ Again, two coders, unaware of the hypotheses, coded 20% of the material. The coders counted which information pieces were present in each transcript and reached an interrater agreement of 89% (Cohen’s $\kappa = .73$). One coder continued coding the rest of the material.

Results

Hypotheses Testing

Strategy use. Nearly all participants ($n = 108$, 90%) reported to have used a strategy during the interview. Almost half of them ($n = 49$, 45.4%) reported a single strategy, while the majority ($N = 59$, 55.6%) stated to have used a combination of two to four different strategies. As can be seen in Table 1, the most frequently reported strategies were *prove capability* (‘Show them that my evidence would hold in court’) and *conceal* (‘Answer as vaguely as possible’). Other reported strategies were *self-presentation* (‘Appear professional and credible’), *explain* (‘Make them understand my difficult situation’), *negotiate* (‘Show willingness to reach an agreement’), and *other* (‘Take over control by asking questions back’). The two strategies that were most often used in combination were *prove capacity* and *conceal* ($n = 32$).

The number of participants who claimed to have used a strategy was the same across interview conditions ($n = 54$ [90%] in both conditions). Chi-square tests did not reveal any significant differences in the extent to which participants in the rapport-based interview condition and the direct interview condition reported to have used the different type of strategies, all $ps < .343$ (Bonferroni corrected). Thus, there was no effect of interview protocol on reported strategy use, meaning that Hypothesis 1 was not supported.

Information provision. Participants were found to be moderately forthcoming, with an average disclosure of 12.74 ($SD = 4.67$) information pieces per person out of the total of 45 pieces (i.e. 28.3%).

An independent *t*-test revealed that participants in the rapport-based interview condition ($M = 13.45$, $SD = 4.93$) and direct interview condition ($M = 12.05$, $SD = 4.37$) did not differ significantly with respect to the amount of information provided, $t(118) = 1.63$, $p = .106$, $d = 0.30$, 95% CI [-0.06, 0.66]. This means that Hypothesis 2 is rejected.

Willingness to enact. To test the effect of the interview on willingness to enact the threat, a 2 (Protocol: direct vs. rapport-based) \times 2 (Time: before interview vs. after interview) mixed ANOVA was performed with participants' willingness ratings as the dependent measure. Cell means are reported in Table 2. No main effect of protocol was found, $F(1, 118) = 0.69$, $p = .407$, $\eta_p^2 = 0.006$, 90% CI [.000, .048]. However, the analysis revealed a main effect of time, $F(1, 118) = 12.79$, $p < .001$, $\eta_p^2 = .098$, 90% CI [.029, .187], indicating that participants were significantly more willing to enact the threat after ($M = 6.35$, $SD = 1.81$) than before the interview ($M = 5.84$, $SD = 1.76$). There was no significant Protocol \times Time interaction, $F(1, 118) = 1.42$, $p = .236$, $\eta_p^2 = .012$, 90% CI [.000, .063]. Thus, the amount of change between before- and after-interview ratings did not differ significantly between the two interview protocols, rejecting Hypothesis 3.

Willingness to interact. To test the effect of the type of interview on participants' willingness to interact with the company, a 2 (Protocol) \times 2 (Time) mixed ANOVA was performed (for cell means, see Table 2). No main effect of interview protocol was found, $F(1, 118) = 0.07$, $p = .794$, $\eta_p^2 = .001$, 90% CI [.000, .024]. However, the analysis again revealed a main effect of time, $F(1, 118) = 30.06$, $p < .001$, $\eta_p^2 = .203$, 90% CI [.104, .303], showing that participants were significantly less willing to interact with the company after ($M = 5.29$, $SD = 2.10$) than before the interview ($M = 6.16$, $SD = 1.78$). There was no significant Protocol \times Time interaction, $F(1, 118) = 2.39$, $p = .626$, $\eta_p^2 = .020$, 90% CI [.000, .078]. Thus, the rate of decline of willingness to interact with the company did not differ between the two interview protocols, rejecting Hypothesis 4.

Exploratory Analyses

The main analyses were conducted for the overall amount of information provided. However, from an applied perspective, some information might be more critical than other information. Hence, 12 raters were asked to read the case and to select the 8 to 12 (out of 45) pieces of information that they considered to be the most critical for assessing the risk that the main character in the case would cause

harm. An independent t -test was conducted with the information pieces that were selected by five or more raters ($n = 15$). On average, participants revealed 5.80 ($SD = 2.19$) out of 15 pieces of this critical information. No significant difference was found between participants in the rapport-based interview condition ($M = 6.07$, $SD = 2.36$) and participants in the direct interview condition ($M = 5.53$, $SD = 2.67$), $t(118) = 1.16$, $p = .248$, $d = 0.21$, 95% CI [-0.15, 0.57].

To examine whether strategy choice influenced the amount and type of information provided, independent t -tests were conducted with respect to the two most frequently reported strategies—*prove capability* and *conceal*. First, participants with the strategy *prove capability* did not provide a significantly different amount of details on the implementation of the threat ($M = 4.39$, $SD = 2.94$) than did participants who did not employ this particular strategy ($M = 3.85$, $SD = 2.57$), $t(118) = 1.07$, $p = .288$, $d = 0.19$, 95% CI [-0.16, 0.55]. Second, the participants who reported to have used the strategy *conceal* provided on average about two details less ($M = 11.64$, $SD = 5.12$) than did participants who did not use this particular strategy ($M = 13.70$, $SD = 4.09$), $t(118) = 2.45$, $p = .016$, $d = 0.45$, 95% CI [0.09, 0.81].

In total, 56 participants reported to have used the strategy *conceal*. Some of these participants ($n = 33$) were vague in their descriptions about what information they withheld (e.g. ‘I left out the important details’), whereas others ($n = 23$) specified which type of information they concealed. The latter group reported to have concealed three types of information: (i) information about persons that could help them implement the threat (e.g. the names of a potential witness, companion, or legal counselor; $n = 19$), (ii) information on their own vulnerability (e.g. emotional or financial problems; $n = 7$), and (iii) specific pieces of evidence (e.g. documentation that proved their argument; $n = 5$). Participants could report to have concealed more than one type of information.

Moreover, the participants who reported to have used the strategy *conceal* were found to be significantly more willing to enact the threat before the interview ($M = 6.29$, $SD = 1.60$) than were the participants who did not report to have used this particular strategy ($M = 5.44$, $SD = 1.81$), $t(118) = 2.69$, $p = .008$, $d = 0.49$, 95% CI [0.13, 0.86]. This finding might imply that those with more serious implementation intentions more often chose to conceal information. However, no correlation was found

between willingness to enact the threat and the amount of information provided, $r = .069$, $p = .455$, 95% CI [-.112, .245].

Finally, we examined to what extent participants' initial attitudes toward enacting the threat and attitudes toward interacting with the conflicting party (before-interview ratings) correlated with their attitudes after the interview. Positive correlations were found between before- and after-interview ratings for willingness to enact the threat, $r = .604$, $p < .001$, 95% CI [.476, .707], and willingness to interact with the conflicting party, $r = .609$, $p < .001$, 95% CI [.482, .711]. In a similar vein, only 21 participants (17.5%) changed the direction of their willingness to enact the threat ($n = 7$ willing to unwilling; $n = 14$ unwilling to willing) after the interview compared to before, and only 29 (24.2%) of the participants changed the direction of their willingness to interact with the conflicting party ($n = 23$ willing to unwilling; $n = 6$ unwilling to willing). A change in direction was counted when participants rated an average value greater than 5 (on a 9-point Likert scale) before the interview, and an average value lower than 5 after the interview—and vice versa. Two 3 (Change: unwilling to willing; willing to unwilling; no directional change) \times 2 (Protocol: direct vs. rapport-based) chi-square tests revealed no significant differences between interview conditions for the number of participants that changed the direction of their willingness to enact the threat, $\chi^2(2, N = 120) = 0.52$, $p = .771$, $\phi = .07$, or to interact with the conflicting party, $\chi^2(2, N = 120) = 0.05$, $p = .973$, $\phi = .02$.

Discussion

Main Findings

The purpose of this study was twofold. First, to learn about threateners' strategies, attitudes, and actual verbal behaviours when being interviewed about their intentions. Second, to examine how different interview styles (direct vs. rapport-based interviewing) may steer these behaviours towards successful interview outcomes. Threatening participants were found to be semi-cooperative. That is, prior to the interview they reported to be willing to discuss their case and provided almost one third of the information they held (and approximately 40% of the critical information they held). In addition to being forthcoming, almost all threateners (90%) reported to have presented their case strategically. The reported use of counter-interview strategies was higher than what is known from research on suspect

interviewing (37% - 60%; Hartwig, Granhag, & Strömwall, 2007), but fits well with previous findings on counter-interview strategy use in threat management interviews (Geurts et al., 2016).

The most frequently used strategies were to emphasise one's capability to enact the threat and to hide information for the interviewer. This finding indicates that threat managers may benefit from interviewing subjects of concern. That is, people who wish to prove their capability need to reveal some information about their planning or preparations. Moreover, people who conceal information by definition withhold knowledge—knowledge that may be elicited by means of skilled interviewing. It is possible that the reported strategies reflected the information-management dilemma that the participants had to navigate (i.e. 'If you tell too much, the company might take advantage of the information you provide. If you tell too little, the company might not take you seriously'). In defense of the paradigm, though, this is a dilemma that real-life threateners often face.

Contrary to the expectations, the study did not support the relative superiority of rapport-based interviewing. No differences were found between protocols for the threateners' strategy use, their information provision, or for their willingness to pursue or discuss the case. These outcomes contrast previous research supporting the efficacy of rapport-based interviewing over accusatorial or direct interviewing (Meissner et al., 2014; Bull, 2013). Two possible explanations for these findings are here suggested. The first is that the manipulation of rapport might not have been powerful enough to cause the predicted effects. The second is that rapport-building approaches might not be better than direct approaches in instrumental conflicts, such as the case scenario that was used in the present study (See also Limitations and Future Research).

The initial attitudes of the interviewees were found to be predictive for the interview outcomes. Interviewees who were relatively more eager to implement the threat (or to interact with the conflicting party) before the interview, were also relatively more eager to do so after the interview. This finding matches a scientific review on motivational interviewing in clinical contexts, showing that the client's attitude (e.g. motivation to change) is a stronger predictor of therapeutic outcomes than the therapist's spirit as such (e.g. empathy or acceptance; Apodaca & Longabaugh, 2009).

Importantly, participants who were initially more positive towards implementing the threat, more often chose to conceal information, and especially information on the actual implementation of the

threat (e.g. names of contact persons, specific pieces of evidence). Placing the finding in a broader perspective, threateners with serious intentions may employ more avoidant strategies than bluffers. This notion fits well with research on suspect interviewing, where guilty interviewees were found to adopt avoidant strategies (e.g. *avoid incriminating details, keep it simple*) more often than innocent interviewees did (Hines et al., 2010; Strömwall, Hartwig, & Granhag, 2006). Differences in counter-interview strategies are presumed to result from different information management needs (i.e. the guilty must conceal the truth, whereas the innocent must reveal the truth), and strategic interview techniques build on such differences (Granhag & Hartwig, 2008).

Furthermore, it was found that regardless of the interview style, interviewing had an escalating, rather than a de-escalating, effect. Threatening participants were more willing to enact the threat after the interview compared to before, and also, they were less willing to interact with the conflicting party after the interview compared to before. Reasonably, these attitude changes may have been a response to the interviewer's rejection of the threateners' demand at the very end of the interview (i.e. 'the company will not pay you'). The impact of the rejection may have overshadowed the nuances of the interview, implying that the mere effect of interview styles are best tested without such a rejection. Yet it is realistic to think that rejections are likely to occur during interactions with people who threaten because their demands or behaviors are often unacceptable. The challenge in crisis communication is therefore to reduce tension, gather information, and work towards a solution, while simultaneously restraining unwanted behavior (Giebels & Taylor, 2010; van der Meer & Diekhuis, 2014). Thus, we argue that any valuable interview methods for threat management need to be effective despite the rejection or restraint that is communicated to the threatener.

Limitations and Future Research

The null findings that were observed when comparing the two interview styles may have been due to methodological limitations. First, the rapport-promoting elements in one of the interview protocols may have been too weak. The pilot study revealed that the rapport-based interview protocol was perceived as more rapport-promoting, compared to the direct interview protocol. Although this difference was significant (with a medium effect size), the ratings did not differ much in absolute terms (i.e. the rapport-based and direct protocols received average ratings of 4.05 and 3.55 on a 7-point scale,

respectively). Moreover, an average score of 4.05 on a 7-point scale suggests that the rapport-based protocol was rapport-promoting only to a moderate extent. This fact, plus the finding that initial counter-interview strategies are difficult to change (Alison et al., 2013; Apodaca & Longabaugh, 2009), suggests that profound means are needed to steer interviewees' behavior. One way forward could be to focus on specific interview techniques (e.g. strategic interview techniques) rather than general interview styles.

Second, the case scenario concerned a work conflict and the interview aim was instrumental (i.e. financial compensation). It has been suggested that instrumental crises, with a typical win-lose structure, are best encountered with rational arguments rather than relational approaches (e.g. being kind, showing empathy; Giebels & Taylor, 2010). A future challenge in experimental research on threat dynamics is to build a paradigm that matches both the reality of the participant as well as the charged nature of threat cases.

On a more general note, it could be argued that one specific type of interviewing—whether it is rapport-based, direct, or strategic—may not be effective in all threat management contexts. This study rested on the assumption that interview styles that are grounded in basic theories of human dynamics are broadly applicable. However, threat managers must deal with a variety of motives, cultures, and mental conditions. Arguably, such background variables should inform the (combination of) interview methods used in a particular case. For instance, communication with stalkers should perhaps focus on restraining the perpetrator's behaviors (Kropp, Hart, Lyon, & Storey, 2011), whereas business-like conflicts are better solved by a rational discussion on the content of the conflict (Giebels & Taylor, 2010). Moreover, building trust may be critical in communication with persons with personality disorders (Bender, 2005), whereas repairing loss of face may be particularly important when interviewing persons from collectivistic cultures (Giebels & Taylor, 2012). In other words, the success of threat management interviewing may depend on the extent to which the interview method fits the case characteristics.

Concluding Remarks

The current findings suggest that threateners are semi-cooperative, which speaks to the importance of skilled interviewing in the field of threat management. No differences in threat management outcomes (i.e. information gain, counter-interview strategies, de-escalation) were found

when comparing direct interviewing with rapport-based interviewing. However, the study showed how threatening interviewees stroke a deliberate balance between proving their stand and disguising implementation details. Especially those with more serious intentions to enact the threat were restrictive in terms of providing information during the interview. Current knowledge on threat management interviewing rests on best practices rather than science. To strengthen the foundation of threat management interviewing, we argue, more experimental research is needed on behaviors that can be expected from the interviewee, and on interview techniques that can exploit these behaviors.

References

- Alison, L. J., Alison, E., Noone, G., Elntib, S., & Christiansen, P. (2013). Why tough tactics fail and rapport gets results: Observing Rapport-Based Interpersonal Techniques (ORBIT) to generate useful information from terrorists. *Psychology, Public Policy, and Law*, 19, 411-431. doi: 10.1037/a0034564
- Alison, L., Alison, E., Noone, G., Elntib, S., Waring, S., & Christiansen, P. (2014). The efficacy of rapport-based techniques for minimizing counter-interrogation tactics amongst a field sample of terrorists. *Psychology, Public Policy, and Law*, 20, 421-430. doi: [10.1037/law0000021](https://doi.org/10.1037/law0000021)
- Apodaca, T. R., & Longabaugh, R. (2009). Mechanisms of change in motivational interviewing: A review and preliminary evaluation of the evidence. *Addiction*, 104, 705-715. doi: [10.1111/j.1360-0443.2009.02527.x](https://doi.org/10.1111/j.1360-0443.2009.02527.x)
- Bender, D. S. (2005). The therapeutic alliance in the treatment of personality disorders. *Journal of Psychiatric Practice*, 11, 73-87. doi: [10.1097/00131746-200503000-00002](https://doi.org/10.1097/00131746-200503000-00002)
- Bull, R. (2013). What is 'believed' or actually 'known' about characteristics that may contribute to being a good/effective interviewer? *Investigative Interviewing: Research and Practice*, 5, 128-143.
- Calhoun, F. S., & Weston, S. W. (2015). Perspectives on threat management. *Journal of Threat Assessment and Management*, 2, 258-267. doi: [10.1037/tam0000056](https://doi.org/10.1037/tam0000056)
- Dalgaard-Nielsen, A. (2013). Promoting exit from violent extremism: Themes and approaches. *Studies in Conflict & Terrorism*, 36, 99-115. doi: [10.1080/1057610X.2013.747073](https://doi.org/10.1080/1057610X.2013.747073)
- Evans, J. R., Meissner, C. A., Brandon, S. E., Russano, M. B., & Kleinman, S. M. (2010). Criminal versus HUMINT interrogations: The importance of psychological science to improving interrogative practice. *The Journal of Psychiatry & Law*, 38, 215-249. doi: [10.1177/009318531003800110](https://doi.org/10.1177/009318531003800110)
- Fein, R. A., & Vossekuil, B. (1998). *Protective intelligence and threat assessment investigations: A guide for state and local law enforcement officials*. Washington, DC: US Department of Justice, Office of Justice Programs, National Institute of Justice.

- Galinsky, A. D., Maddux, W. W., Gilin, D., & White, J. B. (2008). Why it pays to get inside the head of your opponent: The differential effects of perspective taking and empathy in negotiations. *Psychological science*, 19, 378-384. doi.org/10.1111/j.1467-9280.2008.02096.x
- Geurts, R., Ask, K., Granhag, P. A., & Vrij, A. (2016). Eliciting information from people who pose a threat: Counter-interview strategies examined. *Journal of Applied Research in Memory and Cognition*. Advanced online publication. doi: [10.1016/j.jarmac.2016.10.002](https://doi.org/10.1016/j.jarmac.2016.10.002)
- Giebels, E., & Taylor, P. J. (2010). Communication predictors and social influence in crisis negotiations. In R. G. Rogan & F. J. Lanceley (Eds.), *Contemporary theory, research, and practice of crisis/hostage negotiations*. New York, NY: Hampton Press.
- Giebels, E., & Taylor, P. J. (2012). Tuning in to the right wavelength: The importance of culture for effective crisis negotiation. In M. St-Yves & P. L. Collins (Eds.), *The psychology of crisis intervention for law enforcement officers* (pp. 277-294). Montreal, Canada: Éditions Yvon Blais.
- Gill, P. (2015). Toward a scientific approach to identifying and understanding indicators of radicalization and terrorist intent: Eight key problems. *Journal of Threat Assessment and Management*, 2, 187-191. doi.org/10.1037/tam0000047
- Granhag, P. A., Clemens, F., & Strömwall, L. A. (2009). The usual and the unusual suspects: Level of suspicion and counter-interrogation tactics. *Journal of Investigative Psychology and Offender Profiling*, 6, 129-137. doi: [10.1002/jip.101](https://doi.org/10.1002/jip.101)
- Granhag, P. A., & Hartwig, M. (2008). A new theoretical perspective on deception detection: On the psychology of instrumental mind-reading. *Psychology, Crime & Law*, 14, 189-200. doi: [10.1080/10683160701645181](https://doi.org/10.1080/10683160701645181)
- Granhag, P. A., & Hartwig, M. (2015). The Strategic Use of Evidence (SUE) technique: A conceptual overview. In: P.A. Granhag, A. Vrij, & B. Verschuere (Eds.), *Deception detection: Current challenges and cognitive approaches* (pp. 231-251). UK: Wiley Blackwell.
- Granhag, P. A., Kleinman, S. M., & Oleszkiewicz, S. (2016). The Scharff technique: On how to effectively elicit intelligence from human sources. *International Journal of Intelligence and Counter Intelligence*, 29, 132-150. doi: [10.1080/08850607.2015.1083341](https://doi.org/10.1080/08850607.2015.1083341)

- Hartwig, M., Granhag, P. A., & Strömwall, L. A. (2007). Guilty and innocent suspects' strategies during police interrogations. *Psychology, Crime & Law*, 13, 213-227. doi: [10.1080/10683160600750264](https://doi.org/10.1080/10683160600750264)
- Hartwig, M., Granhag, P. A., Strömwall, L. A., & Doering, N. (2010). Impression and information management: On the strategic self-regulation of innocent and guilty suspects. *The Open Criminology Journal*, 3, 10-16. doi: [10.2174/1874917801003010010](https://doi.org/10.2174/1874917801003010010)
- Hartwig, M., Luke, T. J., & Skerker, M. (2016). Ethical perspectives on interrogation. In J. Jacobs & J. Jackson (Eds.), *The Routledge handbook of criminal justice ethics* (pp. 326-347). London and New York: Routledge, Taylor & Francis Group.
- Hines, A., Colwell, K., Hiscock-Anisman, C., Garrett, E., Ansarra, R., & Montalvo, L. (2010). Impression management strategies of deceivers and honest reporters in an investigative interview. *The European Journal of Psychology Applied to Legal Context*, 2, 73-90.
- James, D. V., & Farnham, F. R. (2016). Outcome and efficacy of interventions by a public figure threat assessment and management unit: A mirrored study of concerning behaviors and police contacts before and after intervention. *Behavioral Sciences & the Law*, 34, 660-680. doi: [10.1002/bsl.2255](https://doi.org/10.1002/bsl.2255)
- Justice, B. P., Bhatt, S., Brandon, S. E., & Kleinman, S. M. (2010). *Army field manual 2-22.3 interrogation methods: A science-based review*. Washington, DC (Draft, September).
- Kebbell, M., Hurren, E., & Mazerolle, P. (2006). *An investigation into the effective and ethical interviewing of suspected sex offenders*. Retrieved from Australian Institute of Criminology: <http://crg.aic.gov.au/reports/200304-12.pdf>
- Kropp, P. R., Hart, S. D., Lyon, D. R., & Storey, J. E. (2011). The development and validation of the guidelines for stalking assessment and management. *Behavioral Sciences & the Law*, 29, 302-316. doi: [10.1002/bsl.978](https://doi.org/10.1002/bsl.978)
- Meissner, C. A., Redlich, A. D., Michael, S. W., Evans, J. R., Camilletti, C. R., Bhatt, S., & Brandon, S. (2014). Accusatorial and information-gathering interrogation methods and their effects on true and false confessions: A meta-analytic review. *Journal of Experimental Criminology*, 10, 459-486. doi: [10.1007/s11292-014-9207-6](https://doi.org/10.1007/s11292-014-9207-6)

- Meloy, R. J., Hoffmann, J., Guldinmann, A., & James, D. (2012). The role of warning behaviors in threat assessment: An exploration and suggested typology. *Behavioral Sciences & the Law*, 30, 256-279. doi: [10.1002/bsl.999](https://doi.org/10.1002/bsl.999)
- Meloy, R. J., & Mohandie, K. (2014). Assessing threats by direct interview of the violent true believer. In J. R. Meloy & J. Hoffmann (Eds.), *International handbook of threat assessment* (pp. 388-398). New York, NY: Oxford University Press.
- Milne, B., Shaw, G., & Bull, R. (2007). Investigative interviewing: The role of research. In D. Carson, R. Milne, F. Pakes, K. Shalev & A. Shawyer (Eds.), *Applying psychology to criminal justice* (pp. 65-80). UK: John Wiley & Sons, Ltd.
- O Connor, T., & Carson, W. (2005). Understanding the psychology of child molesters: A key to getting confessions. *Police Chief*, 72, 70-78.
- Oleszkiewicz, S. (2016). *Eliciting human intelligence: A conceptualization and empirical testing of the Scharff technique* (Doctoral dissertation). Retrieved from Gothenburg University: https://gupea.ub.gu.se/bitstream/2077/41567/1/gupea_2077_41567_1.pdf
- Oleszkiewicz, S., Granhag, P. A., & Kleinman, S. M. (2017). Gathering human intelligence via repeated interviewing: Further empirical tests of the Scharff technique. *Psychology, Crime & Law*. Advanced online publication. doi.org/10.1080/1068316x.2017.1296150
- Saywitz, K. J., Larson, R. P., Hobbs, S. D., & Wells, C. R. (2015). Developing rapport with children in forensic interviews: Systematic review of experimental research. *Behavioral Sciences & the Law*, 33, 372-389. doi: [10.1002/bsl.2186](https://doi.org/10.1002/bsl.2186)
- Strömwall, L. A., Hartwig, M., & Granhag, P. A. (2006). To act truthfully: Nonverbal behavior and strategies during a police interrogation. *Psychology, Crime & Law*, 12, 207-219. doi: [10.1080/10683160512331331328](https://doi.org/10.1080/10683160512331331328)
- Tekin, S., Granhag, P. A., Strömwall, L., Giolla, E. M., Vrij, A., & Hartwig, M. (2015). Interviewing strategically to elicit admissions from guilty suspects. *Law and Human Behavior*, 39, 244-252. doi: [10.1037/lhb0000131](https://doi.org/10.1037/lhb0000131)
- Toliver, R. F. (1997). *The interrogator: the story of Hans Joachim Scharff, master interrogator of the Luftwaffe*. Atglen, PA: Schiffer Publishing Ltd.

- Van der Meer, B. B., & Diekhuis, M. L. (2014). Collecting and assessing information for threat assessment. In J. R. Meloy & J. Hoffmann (Eds.), *International handbook of threat assessment* (pp. 54-66). New York, NY: Oxford University Press.
- Vossekuil, B., Fein, R. A., & Berglund, J. M. (2015). Threat assessment: Assessing the risk of targeted violence. *Journal of Threat Assessment and Management*, 2, 243-254. doi: [10.1037/tam0000055](https://doi.org/10.1037/tam0000055)
- Warren, L., Mullen, P., & McEwan, T. (2014). Explicit threats of violence. In J. R. Meloy & J. Hoffmann (Eds.), *International handbook of threat assessment* (pp. 18-38). New York, NY: Oxford University Press.

Table 1

Frequencies of Threateners' Self-Reported Counter-Interview Strategies

Strategy	Total	Interview protocol		χ^2
		Direct	Rapport	
Prove capability	59 (49.2%)	34 (56.7%)	25 (41.7%)	2.70
Conceal	56 (46.7%)	32 (53.3%)	24 (40.0%)	2.14
Self-presentation	27 (22.5%)	9 (15.0%)	18 (30.0%)	3.87
Explain	21 (17.5%)	8 (13.3%)	13 (21.7%)	1.44
Negotiate	9 (7.5%)	5 (8.3%)	4 (6.7%)	0.12
Other	18 (15.0%)	10 (16.7%)	8 (13.3%)	0.26
No strategy	12 (10.0%)	6 (10.0%)	6 (10.0%)	0.00

Note. Threateners could report more than one strategy; thus, percentages do not add up to 100%. The χ^2 values refer to the difference between the direct and rapport-based interview conditions in the proportion of participants who reported the strategy. None of these tests were statistically significant at $p < .05$ (Bonferroni corrected).

Table 2

Means of Before- and After-Interview Ratings as a Function of Interview Protocol

Interview protocol	Willingness to enact		Willingness to interact	
	Before	After	Before	After
Direct	5.87 (1.74)	6.56 (1.68)	6.24 (1.81)	5.29 (2.14)
Rapport	5.80 (1.79)	6.15 (1.93)	6.08 (1.75)	5.28 (2.08)

Note. Both *willingness to enact* and *willingness to interact* were rated on a 9-point Likert scale. Values in parentheses represent standard deviations.

*Appendix A**Instructions to the participant***Background**

Imagine the following scenario. You recently graduated from university and Boston & Company—a leading company in your field— offered you a job. You happily accepted the offer and signed a contract stating that the first half year would be an unpaid internship and after this period, by mutual consent, the contract would be changed into a paid and permanent position.

The internship was demanding and you had worked hard during weekdays, evenings, weekends, and holidays. Your colleagues and the manager appreciated your work. However, to your surprise, the company decided to end your contract after half a year because, according to them, you did not live up to the company's standards in terms of effort and quality of work.

The decision of the company shocked you. Not only did it affect your self-esteem but it also caused you financial problems. You had taken a bank loan to cover your life expenses during the unpaid period. You had never worried about this loan because the company gave you the impression that the permanent contract was just a formality. Suddenly you were unemployed and jobs in your field are scarce.

Now, five months later, you found out via friends that two other young professionals experienced exactly the same at Boston & Company. This information strengthened your idea that the company had mistreated you. As you were newly graduated with little experience of contracts and careers, you felt they tricked you with a false promise and profited from half a year of free labor, while you were left with debts.

You decided to claim a salary for the period that you worked for the company. However, you realise that simply asking for money won't work. You thought that there are two ways to get compensated for your work: i) you press charges with the hope that the court forces the company to pay you, or ii) you make the company believe that you have a strong case, and that they will be willing to pay you the money in order to prevent you from pressing charges.

Additional information concerning your case: i) You kept track of your working hours while you were working for the company. You still have these notes and you calculated that you had worked

an average of 60 hours per week, ii) A former colleague from the company told you that she has access to internal documentation showing that the work you delivered was of excellent quality, iii) Your friend gave you the names of two other persons with similar experiences working for the company, and iv) You have the contact details of a legal counsellor who is specialised in corporate law.

Instructions

You have written a letter to Boston & Company in which you made clear that if they don't retrospectively pay you a salary, you will press charges against them. Boston & Company have received the letter and consulted Robin—an employee working for the Security Unit of Boston & Company—to talk with you about this matter.

You have now 10 minutes to prepare yourself for the talk with Robin. Your ultimate goal is to get your salary payed retrospectively (either by pressing charges or by making them believe that you will press charges), use the interview to achieve this goal. Keep this in mind when talking to Robin; *if you tell too much, the company might use this information against you. If you tell too little, the company might not take you seriously.*

Appendix B

Interview protocols

Direct

[1] My name is Robin. Boston & Company asked me to talk with you about the letter that you have sent us. I would like to ask you a few questions. [2] Could you explain to me how the company decision to end your contract has affected you? [3] Why did you decide to take action now, 5 months later? [4] What do you seek to achieve with this? [5] What exactly are you planning to do? [6] Proceeding with this case will be difficult. How have you prepared for this? [7] Why do you think your case is strong? [8] What will you do if we don't pay you the money? [9] What will you do if you don't win the case in court? [10] I already know that the company will not pay you a salary in retrospect. My advice is to drop the case and accept the situation. [11] I will be your contact person on this matter (business card is offered). You can call me if you have more information or questions concerning your case.

Rapport-based

[1] My name is Robin. Boston & Company asked me to talk with you about the letter that you have sent us. I would like to ask you a few questions *but of course it is your choice whether or not you want to answer those questions*. [2] *I have understood from your letter that you have worked for Boston & Company during a six months internship in which you devoted much time and energy to the company. You were promised a paid and permanent position after the internship but the company ended your contract.* Could you explain to me how this decision has affected you? [3] *The sudden ending of the contract must have come as a surprise for you back then. I understand that you may have felt defeated at first but* why did you decide to take action now, 5 months later? [4] *Just to make sure that I understand you correct,* what is it that you seek to achieve with this? [5] *You don't have to tell me this of course but* what exactly are you planning to do? [6] *I know from my experience working for security units of different companies, that proceeding cases like these can be difficult for the plaintiff, which you are in this case. May I ask you* how you have prepared for this? [7] *I believe that you are a reasonable person. Still, we have to look at the facts,* why do you think that your case is a strong case? [8] What will you do if we don't pay you the money? [9] What will you do if you don't win the case in

court? [10] *I have heard your side of the story and I will report this to the company. But I have to be honest with you.* I already know that the company will not pay you a salary in retrospect *because the contract that you signed doesn't allow for that.* My advice to you is to drop the case and to accept the situation. *As I see it, you are still young and I'm sure that you will face plenty of great career opportunities in the future.* [11] I will be your contact person on this matter (business card is offered). You can call me if you have more information or questions concerning your case.

Note: The Italic phrasings indicate differences between protocols.

*Appendix C**Questionnaire protocol pretesting*

In your role as interviewee, rate your agreement with the following statements (1 = *strongly disagree*; 7 = *strongly agree*)

1. The interviewer's approach is friendly
2. The interviewer wants to know what I have to say
3. The interviewer is confrontational
4. The interviewer understands the difficult situation that I am in
5. The interviewer is trying to get the best outcome for both of us
6. I can choose not to answer a question and the interviewer would respect that
7. The interviewer is judgmental
8. I can share the problems I have with my former employer and the interviewer would want to listen to this
9. The interviewer lacks understanding of my situation
10. The interviewer would accept my answers even if he would disagree with them
11. I think that the interviewer is able to see the situation from my point of view
12. The interviewer fails to take my perspective
13. The interviewer wants to help me out of this difficult situation

Appendix H: Manuscript Study IV

Received: 10 October 2016 | Revised: 12 May 2017 | Accepted: 18 June 2017

DOI: 10.1002/jip.1486

WILEY

RESEARCH ARTICLE

Assessing threats of violence: Professional skill or common sense?

Renate Geurts^{1,2}  | Pär Anders Granhag^{1,3} | Karl Ask¹ | Aldert Vrij²¹University of Gothenburg, Gothenburg, Sweden²University of Portsmouth, Portsmouth, England³Norwegian Police University College, Oslo, Norway

Correspondence

Renate Geurts, Department of Psychology, University of Gothenburg, P.O. Box 500, 405 30 Gothenburg, Sweden.
Email: renate.geurts@psy.gu.se

Funding information

Erasmus Mundus Joint Doctoral programme in Legal Psychology (EMJD-LP)

Abstract

When faced with threats of violence, it is of great importance to assess the risk for actual harm to occur. Over the last decades, this task has developed into a domain of its own and professionals have specialised in *threat assessment*. However, it is yet unknown whether professional experience affects the quality of threat assessments. The present study examined how threat assessment professionals ($N = 44$), university students ($N = 44$), and laypersons ($N = 45$) assessed the risk for violence in three fictitious cases. The assessments (i.e., assigning risk values to different pieces of information) were found to be strikingly similar across the three groups. Yet, professionals agreed more with one another on their assessments, and professionals identified more relevant (empirically supported) threat cues when given the opportunity to request additional information. These results suggest that threat assessment professionals know better than nonprofessionals what information to look for, and hence, they may contribute most in the process of gathering information to clarify the threat. Such knowledge can help to optimise the use of expertise, which may improve the quality of threat assessments. The current findings can be of value to those who consult threat assessment professionals, as well as to the professionals themselves.

KEYWORDS

decision making, expert performance, threat assessment, threat management, violence risk

1 | INTRODUCTION

The 9/11 attacks and subsequent mass killings in Western societies brought about a growing awareness of risks and security, and the field of threat assessment has developed rapidly since. Threat assessment is the process of information gathering to understand and evaluate a threat of violence (Meloy, Hoffmann, Roshdi, Glaz-Ocik, & Guldinann, 2014a). Developments in this field are evidenced by a fair amount of research examining cases and classifying warning behaviours (e.g., Dietz & Martell, 2010; Hoffmann, Meloy, Guldinann, & Ermer, 2011). Such research has resulted in

jargon (e.g., “intended violence”; Calhoun & Weston, 2003), in guidelines on how to conduct threat assessment investigations (e.g., Fein & Vossekuil, 1998), and in threat assessment tools (e.g., James, MacKenzie, & Farnham, 2014; White & Meloy, 2010). Importantly, the growing body of knowledge has allowed practitioners to specialise, and associations have been established for so-called *threat assessment professionals* (e.g., the Association of European Threat Assessment Professional, AETAP).

Threat assessment professionals must mitigate the risk that individuals who pose threats of violence will indeed commit violence. One of their key tasks is to identify conditions and behaviours that precede planned acts of violence (Meloy et al., 2014a; Skeem & Monahan, 2011). The present study investigates how professionals and nonprofessionals assess (fictitious) threats of violence. The aim of this study is to identify threat assessment tasks for which professional experience is more or less critical. Such an understanding is important because allocating expertise to tasks that could be done by others would be inefficient, and relying on laypersons' knowledge when expertise is needed can be fatal.

A study on threat assessment professionals demands a brief outline of how this profession is practiced, and what professionals are expected to contribute. The methodology used in threat assessment largely resembles violence risk assessment, in which risk factors are used to estimate the likelihood of physical violence occurring in a population (Skeem & Monahan, 2011). Risk assessment and threat assessment are professional fields that share the same goal: to assess and manage risks for violence. However, threat assessors and risk assessors *typically* operate in different contexts (law enforcement vs. health care, resp.), which results in different responsibilities (operational vs. legal decision making). For an overview of differences and similarities in threat and risk assessment, see Meloy et al. (2014a). Most relevant to the present study is the fact that both fields make use of a *structured professional judgment* model (SPJ; Guy, Packer, & Warnken, 2012). SPJ relies on the discretion of the professional, while providing structure to their judgment via empirically informed guidelines (Douglas, Ogloff, & Hart, 2003). SPJ combines aspects of two decision-making models that characterise risk assessment practices: the unstructured *clinical* model that relies on the subjective assessment of the expert and the highly structured *actuarial* model that relies on data based algorithms (Meehl, 1954). Risk assessment instruments that are developed under an SPJ approach hold a list of risk and protective factors that have been identified by a literature review. These factors are operationalised, and guidelines are provided on how to score them. However, the scores do not add up to a fixed outcome but they are meant to guide the professional in their clinical judgement of risk (Douglas et al., 2003). The responsibility of professionals applying SPJ is to recognise potential risk or protective factors in an individual case and to assess the degree to which the (combination of) factors increase or decrease the overall risk for violence (Douglas et al., 2003; Skeem & Monahan, 2011). In other words, threat assessment professionals are supposed to both *select* and *weight* information cues to indicate the risk for violence posed by the individual of concern. But how good are they in doing so?

The quality of expert performance can be defined by the ability to perform consistently with oneself and with others (i.e., reliability) and by the ability to base decisions on relevant information (i.e., biasability; Dror, 2016). Differently put, experts are presumed to identify, cluster, and weight information in the same way, and they should make their judgments relatively free of biases (Einhorn, 1974). As it remains challenging to certify expertise (Ericsson, 2008; Shanteau, Weiss, Thomas, & Pounds, 2002), the focus of this paper is on the more objective measure of *professional experience*. Specifically, we examined how professional experience affects the assessment of threats of violence.

Research suggests that superior professional performance results mainly from domain-specific knowledge (Patel & Groen, 1986; Schmidt & Rikers, 2007). Such knowledge allows professionals to quickly recognise relevant patterns and to generate scenarios, which contributes to an efficient information search (Elstein & Schwarz, 2002). Expert physicians, for instance, were found to be significantly faster than novices producing diagnostic hypotheses (Joseph & Patel, 1990). More recently, in a study with British police officers, experienced detectives generated more investigative hypotheses and actions when presented with a missing-person case, compared to their less experienced colleagues (Fahsing & Ask, 2016).

The literature on risk perception further suggests that experts have a more realistic sense of the likelihood for danger to occur, whereas the general public tends to overestimate infrequent but catastrophic events (e.g., a terrorist attack; Weber, 2001). However, this difference in knowledge between experts and laypersons does not necessarily

influence how they weight risk cues when faced with them. Simply illustrated, an expert might assess the overall risk for a terror attack to occur as being low, but when confronted with concrete signs of an attack (e.g., someone enters the airport wearing a bomb vest), both experts and novices will judge this information as similarly dangerous. It has been theorised that risk assessment is largely affective in nature—even when approached rationally—and that affective risk assessment is equally well (or poorly) developed in experts and novices, as responding to threats is deeply rooted in human evolution (Slovic, Finucane, Peters, & MacGregor, 2004; Slovic & Weber, 2002). Studies that examined people's capability to detect suspicious behaviour showed that professionals were no better than novices in detecting deceit (Bogaard, Meijer, Vrij, & Merckelbach, 2016; DePaulo & Pfeifer, 1986), or in deciding which travellers should undergo customs inspection (Kraut & Poe, 1980). Thus, research and theory suggest that professionals may know better what information to look for, but once provided with the correct information cues, professionals and nonprofessionals may assess this information similarly.

Based on this notion, we had no reason to expect that professional experience would affect the ability to distinguishing risk factors from neutral factors, or from protective factors. However, it was presumed that professional experience would affect the level of interrater-agreement, meaning that professionals who examine the same information reach the same conclusion. Thus, we predicted that professionals would agree with one another on their risk assessments to a higher extent than nonprofessionals would (Hypothesis 1). Furthermore, professionals were expected to know what information to look for. Therefore, we predicted that the professionals' (vs. nonprofessionals') search for information would be comparatively more in line with empirically supported threat cues (Hypothesis 2).

2 | METHOD

2.1 | Participants and design

One hundred forty-one participants completed the survey. The sample consisted 45 professionals (30 men, 15 women, $M_{age} = 44.87$ years, $SD = 10.13$ years), 46 university students (12 men, 34 women, $M_{age} = 27.42$ years, $SD = 9.97$ years), and 50 laypersons (19 men, 31 women, $M_{age} = 42.48$ years, $SD = 13.01$ years). The sample size was guided by the number of professionals that could be recruited, meaning that the number of students and laypersons was matched with the number of professionals that participated. The reason for including two nonprofessional samples (students and laypersons) was that students may not fully represent the nonprofessional population, as they are studying to become professionals themselves. Working experience in threat assessment averaged 12.70 years ($SD = 8.96$) in the professional sample. One participant in the professional sample reported to have just 1 year of working experience in threat assessment and seven participants in the nonprofessional samples reported to have more than 1 year of working experience in threat assessment. The data of these eight individuals were excluded from further analyses. One hundred and thirty-three participants remained, of which 44 professionals (30 men, 14 women, $M_{age} = 45.23$ years, $SD = 9.95$ years), 44 students (12 men, 32 women, $M_{age} = 26.53$ years, $SD = 8.63$ years), and 45 laypersons (17 men, 28 women, $M_{age} = 42.09$ years, $SD = 12.80$ years).¹

Professionals were approached via associations of threat assessment professionals in Europe (Association of European Threat Assessment Professionals, AETAP) and in Canada (Canadian Association of Threat Assessment Professionals, CATAP) to take part in a survey on threat assessment. They were either members of these associations, attended a conference on threat assessment in April 2016 that was organised by AETAP, or they were recommended as eligible participants by those who were initially approached. The countries in which the professionals operated were Canada ($n = 9$), The Netherlands ($n = 8$), Germany ($n = 7$), the United States ($n = 3$), Australia ($n = 3$), worldwide ($n = 3$), Austria, Belgium, Hong Kong, Luxembourg, New Zealand, South-Africa, Sweden, and Switzerland (all $n \leq 2$). Professionals were not financially rewarded for their participation.

Students were approached via the participant pool of a Swedish university where they had signed up for participation in psychological research. They were compensated 50 SEK (approx. 6 dollar). Laypersons were

approached online through Amazon's Mechanical Turk and were paid 0.30 USD upon completion. Participants in the laypersons sample were from the United States ($n = 41$) and India ($n = 9$). All participants completed the same survey. The data collection took place from April to June 2016.

2.2 | Materials

Three fictitious cases were constructed in which a person posed a potential threat of violence towards one or several other persons. To prevent the outcomes from being the result of one particular case or one particular domain of violence, each case reflected a different domain of violence that is commonly encountered by threat assessment professionals. These domains were intimate partner violence (case "Terry"), public figure violence (case "Marc"), and workplace violence (case "Frank"). The cases consisted of 15 to 21 information cues describing (a) the context in which the threat evolved and (b) the behaviours and characteristics of the person posing the threat. Each information cue in the cases was selected based on risk factors and protective factors that have been found to be empirically valid. For instance, the information cue *Frank's position within the firm is uncertain* reflected the risk factor "employment instability" (Feldman & Johnson, 1996). Protective factors are conditions and behaviours that may reduce the risk of violence, which can also be the absence of risk factors (Borum, 2000). For instance, the information cue *Frank joins a running group twice a week* indicated the absence of the risk factor "social isolation" (Meloy, White, & Hart, 2013). In addition to the risk and protective factors, each case held two pieces of neutral information. That is, information that is not empirically known to increase or decrease the risk for violence as such (e.g., having tattoos). Two experienced threat assessment professionals provided feedback on the cases. They recognised the cases as cases they would encounter in their profession and hence perceived the storylines as relevant and realistic. The cases are presented in Appendix A.

2.3 | Procedure

The first page of the survey stated that the study included three descriptions of separate cases in which a person poses a potential threat. The participants were instructed to read each case and to answer the accompanying questions. Participants were informed that participating was confidential, voluntary, and for research purposes only. After agreeing on these terms, they were presented with the first case, followed by three questions. First, participants were asked to assess the overall risk for physical violence currently posed by the main character (0% = *no risk for violence*, 100% = *guaranteed risk for violence*; any number between 0 and 100 could be selected). Next, they were presented with a list of specific information cues derived from the case. They were asked to assess the extent to which each information cue increased or decreased the risk for violence in this particular case (e.g., *Frank's position within the firm is uncertain*; $-4 = \text{very strong decrease}$, $0 = \text{neutral}$, $4 = \text{very strong increase}$). Finally, participants were asked to list up to five additional information cues that they would request in order to make a more adequate assessment of the risk for violence for this particular case. The same procedure was repeated for each case. The cases were presented in a randomised order.

After completing the case-related questions, participants provided their age, gender, and number of years working in the field of threat assessment. In addition, professionals were asked to indicate in which country they worked and how they were professionally involved in threat assessment (e.g., screening and security; criminal intelligence gathering). Students and laypersons were asked to indicate their country of residence and their employment status (e.g., student; employed for wages). Participants needed approximately 30 min to complete the survey.

2.4 | Data analyses

2.4.1 | Coding

Two research assistants coded the information cues requested by the participants. First, the total number of requested information cues was counted per participant per case (ranging from 1 to 5). Second, each information

request was classified as “key request” or “other request.” A request was considered a “key request” when it matched one of the 11 key questions identified by Vossekuil, Fein, and Berglund (2015). These key questions are supposed to cover all areas that should be inquired in order to make a fully informed assessment about a person posing a threat. Information requests that did not fit any of the key questions were categorised as “other request.” The “other requests” were then further qualified into specific areas of inquiry. All areas of inquiry specifying “key requests” and “other requests” are listed in Table 1. Two coders categorised a random 30% of the material into “key requests” versus “other requests” (85.71%, Cohen's $\kappa = .71$) and further specified the requests into one of 17 specific areas of inquiry (74.44%, Cohen's $\kappa = .66$). One coder completed codings on the remaining material.

2.4.2 | Recoded values

Participants assessed the information in the cases on a 9-point scale with values ranging from -4 to $+4$. These values were chosen to enhance the participants' visual representations of risk decrease (minus) and risk increase (plus). However, the scale was recoded into values ranging from 1 to 9 for data analyses.

3 | RESULTS

3.1 | Initial analyses of risk assessments

To reiterate, the assignment of a risk value (1 = *very strong decrease*, 9 = *very strong increase*) to one information cue was considered one assessment. The three cases together contained 57 information cues. Hence, each participant made 57 assessments of specific information cues. One-sample t tests revealed that professionals assessed information cues that reflected risk factors as risk increasing (i.e., the average rating was significantly higher than the neutral value “5”; $M_{\text{professional}} = 6.44$, $SD = 0.56$, $t(43) = 17.14$, $p < .001$, $d = 5.17$) and information cues that reflected

TABLE 1 Areas of inquiry used to classify requested information

Key requests (Vossekuil et al., 2015)

1. What are the subject's motives and goals?
2. What has the subject communicated about his or her intentions to anyone (target, law enforcement, family, friends, colleagues, associates, and/or diary/journal)?
3. Is there evidence that the subject has engaged in attack-related behaviours?
4. Is there evidence that the subject has engaged in menacing, harassing, and/or stalking type behaviour?
5. Does the subject have a history of mental illness involving command hallucinations, delusional ideas, feelings of persecution, and so forth, with indications that the subject has acted on those beliefs?
6. How organised is the subject? Does the subject have the ability to plan and execute a violent action?
7. Is there evidence that the subject is experiencing feelings of hopelessness, desperation, or despair?
8. Is what the subject says consistent with his or her actions?
9. Does the subject see violence as acceptable, desirable, or the only way to solve problems?
10. What concerns do those who know the subject have about the subject's behaviour?
11. What factors in the subject's life and/or environment could change and thereby increase the subject's risk of attacking? What factors could change and thereby decrease the risk posed?

Other requests

1. Requests about upbringing
2. Requests about criminal records that do not concern violence or stalking
3. Requests about drugs, alcohol and medication that do not concern mental illness
4. Requests about protective factors that do not concern the future
5. Requests about finances without a specified reason for the request
6. Requests that do not fit any of the previous categories

protective factors as risk decreasing (i.e., the average rating was significantly lower than the neutral value "5"; $M_{\text{professional}} = 3.90$, $SD = 0.74$, $t(43) = 9.93$, $p < .001$, $d = 2.99$). Information cues that reflected neither risk factors nor protective factors were rated as neutral (i.e., the average rating was statistically similar to the neutral value "5"; $M_{\text{professional}} = 4.97$, $SD = 0.48$, $t(43) = 0.45$, $p < .652$, $d = 0.14$). Students and laypersons made ratings similar to those of professionals for risk factors ($M_{\text{student}} = 6.31$, $SD = 0.56$, $t(43) = 15.37$, $p < .001$, $d = 4.63$; $M_{\text{layperson}} = 6.05$, $SD = 0.98$, $t(44) = 7.18$, $p < .001$, $d = 2.14$) and for protective factors ($M_{\text{student}} = 4.16$, $SD = 1.06$, $t(43) = 5.27$, $p < .001$, $d = 1.59$; $M_{\text{layperson}} = 3.86$, $SD = 1.25$, $t(44) = 6.01$, $p < .001$, $d = 1.79$). However, the neutral cues were rated as neutral by laypersons ($M_{\text{layperson}} = 4.72$, $SD = 1.27$, $t(44) = 1.44$, $p = .156$, $d = 0.43$) but as risk decreasing by students ($M_{\text{student}} = 4.49$, $SD = 1.34$, $t(43) = 2.56$, $p = .014$, $d = 0.78$).

The mean values for each information cue are displayed in Figure 1. As shown in the figure, the professionals' assessments were highly similar to the assessments of the nonprofessionals. Only two out of 57 information cues were assessed in one direction by professionals (risk decrease) and in the other direction by nonprofessionals (neutral/risk increase). Although this could have been the result of chance, the two items (*Rebecca has avoided all contact with Terry* and *Rebecca has received a new telephone number and moved to another neighbourhood*) reflected a

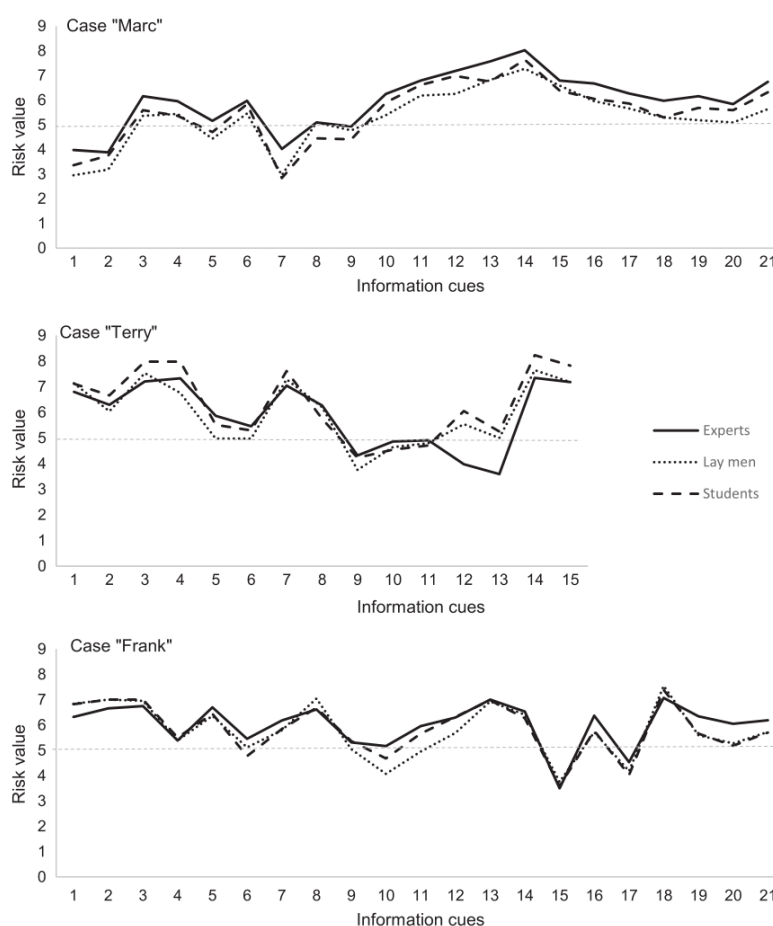


FIGURE 1 Risk assessments (1 = very strong risk decrease, 9 = very strong risk increase) that professionals, students, and laypersons made for the information cues presented per case

similar theme, which was contact between victim and threatener in partner violence. Furthermore, participants in all three samples assigned the highest risk values to information cues that reflected a communicated threat.

Besides assessing specific information cues, participants were asked to judge the *overall* risk for violence for each case (0% = *no risk*, 100% = *guaranteed risk*). A 3 (Sample: professionals vs. students vs. laypersons) \times 3 (Case: Terry vs. Marc vs. Frank) mixed analysis of variance (ANOVA) was performed on the violent risk ratings, with sample as the between-subjects factor. The descriptive statistics are reported in Table 2. The analysis yielded a significant Sample \times Case interaction effect, $F(4, 256) = 4.01, p = .004, \eta_p^2 = .059$. Tests of simple effects revealed different risk assessments across samples for case "Terry," $F(2, 128) = 10.09, p = <.001, \eta_p^2 = .136$. Professionals judged the overall risk for violence lower than did students ($p < .001$) and laypersons ($p = .001$). No difference was found between students and laypersons ($p = .329$). Furthermore, no differences across samples were found for case "Mark," $F(2, 128) = 0.24, p = .784, \eta_p^2 = .004$, or for the case "Frank," $F(2, 128) = 1.59, p = .208, \eta_p^2 = .024$.

3.2 | Hypotheses testing

3.2.1 | Agreement

Agreement among assessors becomes apparent in the standard deviation of their ratings, with the lower the standard deviation, the more similar the ratings. A 3 (Sample: professionals vs. students vs. laypersons) \times 3 (Case: Terry vs. Marc vs. Frank) between-items ANOVA was conducted on the standard deviations for the information cues. A main effect for sample occurred, $F(2, 162) = 106.67, p < .001, \eta_p^2 = .568$. Planned contrasts showed that the average standard deviation within the professional sample ($M = 1.14, SD = 0.21$) was significantly lower than the average standard deviation within the student sample ($M = 1.48, SD = 0.26, p < .001$) and the layperson sample ($M = 1.75, SD = 0.91, p < .001$). Post hoc test further revealed that the difference between the student sample and the layperson sample was significant too ($p < .001$). The main effect of case was not statically significant, $F(2, 162) = 0.52, p = .598, \eta_p^2 = .006$, neither was the Sample \times Case interaction effect, $F(4, 162) = 1.51, p = .200, \eta_p^2 = .036$. Thus, the results indicate that the consensus among the professionals was systematically (i.e., regardless of the case) higher than the consensus among the nonprofessionals. This supports Hypothesis 1.

The above analysis does not account for where on the 9-point scale the spread was located. Spread on the lower (1–3), central (4–6), or higher part (7–9) of the scale was weighted equally. However, when examining agreement using this scale, the spread on the central part may be particularly relevant because it contains both a risk decreasing value (4) and a risk increasing value (6). More specific, agreement on the *direction of risk* (i.e., increase or decrease) can be considered more critical than agreement on the magnitude of risk (e.g., strong increase or very strong increase). To test for differences between samples in agreement on direction, a chi-square test was performed on the number of confidence intervals within each sample that included the central value of the scale ("5"). Confidence intervals containing the middle value imply that some participants in the sample rated the information as risk decreasing (values below 5), whereas others in the sample rated the same information as risk increasing (values above 5). The six neutral information cues were excluded from the analysis because these cues were expected to obtain ratings close to the value of 5. The analysis was conducted on the assessments of the remaining 51 information cues. A significant difference across samples was found with regard to the number of confidence intervals containing the value 5, $\chi^2 (2, N = 153) = 8.70, p = .013, \phi = .24$. Thus, in further support of Hypothesis 1, professionals rarely disagreed with each

TABLE 2 Mean percentages for violence risk per case judged by professionals, students, and laypersons

	Professionals	Students	Laypersons
Case "Marc"	43.05% (20.17)	46.11% (20.75)	43.56% (24.54)
Case "Terry"	57.83% (23.84)	76.07% (17.29)	71.98% (17.53)
Case "Frank"	48.62% (23.87)	47.73% (22.25)	55.44% (20.89)

Note. Mean percentages are based on a rating scale ranging from 0% (*no risk for violence*) to 100% (*guaranteed risk for violence*). The numbers in parentheses represent standard deviations.

other on whether information should be assessed as risk increasing or risk decreasing ($N = 3$, 5.9%), whereas such disagreement among laypersons occurred in approximately one third of the assessments made ($N = 14$, 27.5%, $p < .05$). The frequency of disagreement among students ($N = 8$, 15.7%) was not found significantly different from the other two samples.

3.2.2 | Information search

After assessing the risk for violence, participants were asked to list up to five additional information cues that they considered relevant for making a more adequate assessment. The requested information cues were classified into "key requests" and "other requests" and further divided into different areas of inquiry (see Section 2.4.1). ANOVAs were conducted for each case on (a) the total number of information requests, (b) the number of "key requests," (c) the number of "other requests," and (d) the number of different areas that were inquired. The latter measure served as an indication for the variety of the requested information. Descriptive and inferential statistics are presented in Table 3. Planned contrasts confirmed Hypothesis 2. Professionals requested significantly more key information than students (all cases $p < .001$) and laypersons did (all cases $p < .001$). Furthermore, requests that were made by professionals covered significantly more different areas of inquiry compared to request made by students (all cases $p < .001$) and laypersons (all cases $p \leq .001$). Post hoc tests showed no differences between students and laypersons on any of the measures. Thus, when given the opportunity to gather additional data, professionals requested comparatively more relevant information and from a comparatively wider variety of domains.

4 | DISCUSSION

The results demonstrate that threat assessment professionals agreed more with one another on their risk assessments compared to nonprofessionals. Furthermore, professionals requested comparatively more relevant information (i.e., information that was consistent with empirical threat cues), and they based their risk assessment on more different types of information. Both the relevance and the variety of the information gathered relate to the quality of threat assessments (Fein & Vossekuil, 1998). On a more general level, empirically supported decision

TABLE 3 Means and inferential statistics for the analyses of the requested information

Measure	Professionals	Students	Laypersons	<i>F</i>	<i>p</i>	η_p^2
Case "Marc"						
No. of information pieces requested	3.66 (1.55)	2.16 (1.60)	2.56 (1.67)	10.27	.000	.136
"key requests"	2.68 (1.63)	1.18 (1.08)	1.62 (1.13)	15.42	.000	.192
"other requests"	0.98 (1.00)	0.95 (1.18)	0.93 (1.23)	0.02	.984	.000
No. of areas inquired	3.23 (1.46)	1.86 (1.31)	2.13 (1.34)	12.24	.000	.158
Case "Terry"						
No. of information pieces requested	3.91 (1.54)	2.11 (1.70)	2.51 (1.53)	14.68	.000	.185
"key requests"	2.64 (1.63)	1.07 (1.19)	1.22 (0.97)	22.70	.000	.260
"other requests"	1.27 (1.11)	1.05 (1.16)	1.29 (1.49)	0.25	.779	.004
No. of areas inquired	2.95 (1.40)	1.64 (1.33)	1.91 (1.02)	12.46	.000	.162
Case "Frank"						
No. of information pieces requested	3.82 (1.72)	2.27 (1.48)	2.49 (1.62)	11.93	.000	.155
"key requests"	2.64 (1.54)	1.34 (1.12)	1.56 (1.16)	12.84	.000	.165
"other requests"	1.18 (1.24)	0.98 (1.30)	0.93 (1.16)	0.51	.602	.008
No. of areas inquired	3.11 (1.56)	2.00 (1.24)	2.09 (1.26)	9.15	.000	.123

Note. The numbers in parentheses represent standard deviations.

making as well as interrater agreement reflect quality standards in expert performance (Dror, 2016; Einhorn, 1974). Hence, the results suggest that domain-specific experience advances threat assessment practices. With that said, professionals' beliefs about what cues were (and were not) alarming were highly similar to nonprofessionals' beliefs, suggesting that the actual interpretation of information in threat cases may be rather intuitive.

The current findings fit well in the state of science on expert performance. Early theories proposed that expert knowledge is more critical for cue selection (i.e., what information should be looked for) than for cue weighting (i.e., how should the information be interpreted; Dawes, 1979; Einhorn, 1974). Advanced performers, ranging from chess grandmasters to cardiologists and intelligence analysts, have been found to be particularly good at extracting a meaningful gist from larger sets of data (Corbin, Reyna, Weldon, & Brainerd, 2015; De Groot, 1978; Reyna & Lloyd, 2006). In other words, their experience directs their attention to critical information. When interpreting this information, however, studies have shown that professionals, just like laypersons, often rely on common sense (Masip, Herrero, Garrido, & Barba, 2011; Stolper et al., 2011). Drawing more specifically on literature on risk perception, it has been theorised that people rely on two systems when they assess risk in financial, health, and safety domains: an affective system and a cognitive system (Slovic et al., 2004). The cognitive system contains, among others, knowledge on probabilities of danger to occur and is better developed in experts than in novices (Weber, 2001), whereas the affective system, containing emotional reactions to risk, is inherently present and equally developed in all humans. Although the two systems operate simultaneously, the affective response to risk is assumed to be dominant (Damasio, 2001; Slovic et al., 2004). This theory might explain why common sense notions on risk can overrule expert knowledge when assessing threats of violence. However, the role of affect in professional threat assessment yet needs to be investigated.

The consensus found among professionals is to some extent reassuring. It suggests that threat assessment professionals tend to reach similar conclusions when assessing the same case. This sheds a positive light on threat assessment practices, as research on other legal domains reveals that disagreement among professionals is not uncommon. For instance, forensic experts were found to produce inconsistent interpretations with regard to DNA evidence (Dror & Hampikian, 2011), fingerprints (Ulery, Hicklin, Buscaglia, & Roberts, 2012), and footwear (Majamaa & Ytti, 1996). Although such inconsistencies are worrisome, it should be acknowledged that consistent interpretations are not necessarily accurate. Whether the professionals' judgments for the current study were accurate or not could not be established given that fictitious cases were used. Yet, their judgments matched the risk and protective factors that are known from the literature, which speaks to the quality of their assessments.

4.1 | Limitations and future research

The study is limited in ways that might be addressed in future research. First, there is no guarantee that the information cues in the cases are directly tied to one particular factor, whether risk, neutral, or protective. For instance, suffering from diabetes was included as a neutral factor because diabetes has never been proven to relate to the enactment of threats. However, a participant could have reasoned that suffering from a chronic disease is a stressful condition and should thus be assessed as information that is risk increasing. Such reasoning would be in line with research showing that personal stressors may indeed indicate a higher risk for violence (Meloy et al., 2013). As the current study did not tap into the participants' reasoning behind their assessments, it remains unknown if (and if so, how) participants connected the information cues to possible risk factors.

Another potential concern is that the cues in the cases may have been self-evident, meaning that their interpretation was straightforward. For example, the cue *Marc is highly frustrated that the Minister has not replied*. It is quite clear that frustration is risk increasing rather than risk decreasing. If the information cues in this study were less ambiguous than the information cues threat assessors typically face in real life, this may form an alternative explanation for the similarities found between the professionals and nonprofessionals. With that said, measures were taken to mitigate the risk of biased materials. The cases were perceived as realistic by two experienced threat assessment professionals, and the cases contained risk factors known from the literature on threat assessment. Future studies

could address potential limitations in the materials by more extensive pretesting and/or by studying threats assessors in a naturalistic setting. Naturalistic decision making (NDM) research has provided valuable insights on how to improve professional performances (Klein, 2008). The domain of threat assessment suits the NDM characteristics well, as threat assessors—just like criminal investigators—typically operate in an uncertain and dynamic environment in which the stakes are high and time is limited (Ask & Alison, 2010).

A brief note is warranted on a possible bias in the professional sample. Professionals may have been more motivated participants compared to nonprofessionals as the study concerned their own field of expertise. This could explain the higher number of information requests on behalf of the professionals. Yet, motivation does not explain the higher number of *relevant* information requests made by the professionals. The latter may still be best explained by their professional experience.

The present study solely focussed on threat assessment but the responsibilities of threat assessment professionals typically also involve *threat management* (Meloy, Hart, & Hoffmann, 2014b). Threat management refers to violence prevention and concerns questions such as: What action should be taken to mitigate the threat? Who should be involved in such action? And, how should the case be monitored? Future research might profit from examining how professional experience affects threat management tasks.

Taken together, the current study did not mirror the full dynamics and complexity of threat assessment work. However, the controlled and systematic set-up of the study holds great value because it allows for normative conclusions (i.e., “Outcome A is more/better than outcome B”) rather than mere descriptive outcomes. Such a semi-experimental approach is novel to the field of threat assessment and it may contribute to a stronger scientific base.

4.2 | Contribution to the field

The current findings indicate that threat assessment professionals may contribute most with tasks pertaining to *information gathering*. Professionals may advance the information search by setting the right scope, filtering diagnostic cues from less relevant information, and recognising what intelligence is still missing. The field of threat assessment can benefit from such knowledge in three important ways. First, those who consult threat assessment professionals can make more deliberate decisions when allocating responsibilities and resources. Second, the professionals can better explain to their clients what may be expected of them. Third, and most important, having the right person on the right job improves the quality of threat assessments, which should ultimately result in a safer society.

ACKNOWLEDGMENT

This research was funded by the Erasmus Mundus Joint Doctoral programme in Legal Psychology (EMJD-LP).

ENDNOTE

¹ Gender and age, when included as covariates in statistical analyses, did not change the pattern of the results and will be disregarded in the reported analyses.

REFERENCES

- Ask, K., & Alison, L. (2010). Investigators' decision making. In P. A. Granhag (Ed.), *Forensic psychology in context: Nordic and international perspectives* (pp. 35–55). Cullompton, UK: Willan.
- Bogaard, G., Meijer, E. H., Vrij, A., & Merckelbach, H. (2016). Strong, but wrong: Lay people's and police officers' beliefs about verbal and nonverbal cues to deception. *PloS One*, 11. <https://doi.org/10.1371/journal.pone.0156615>
- Borum, R. (2000). Assessing violence risk among youth. *Journal of Clinical Psychology*, 56, 1263–1288. [https://doi.org/10.1002/1097-4679\(200010\)56:10<1263::AID-JCLP3>3.0.CO;2-D](https://doi.org/10.1002/1097-4679(200010)56:10<1263::AID-JCLP3>3.0.CO;2-D)
- Calhoun, F. S., & Weston, S. W. (2003). *Contemporary threat management: A practical guide for identifying, assessing, and managing individuals of violent intent*. San Diego, CA: Specialized Training Services.

- Corbin, J. C., Reyna, V. F., Weldon, R. B., & Brainerd, C. J. (2015). How reasoning, judgment, and decision making are colored by gist-based intuition: A fuzzy-trace theory approach. *Journal of Applied Research in Memory and Cognition*, 4, 344–355. <https://doi.org/10.1016/j.jarmac.2015.09.001>
- Damasio, A. R. (2001). Emotion and the human brain. *Annals of the New York Academy of Sciences*, 935, 101–106. <https://doi.org/10.1111/j.1749-6632.2001.tb03475.x>
- Dawes, R. M. (1979). The robust beauty of improper linear models in decision making. *American Psychologist*, 34, 571–582. <https://doi.org/10.1037/0003-066X.34.7.571>
- De Groot, A. D. (1978). *Thought and choice in chess* (2nd ed.). The Hague: Mouton Publishers.
- DePaulo, B. M., & Pfeifer, R. L. (1986). On-the-job experience and skill at detecting deception. *Journal of Applied Social Psychology*, 16, 249–267. <https://doi.org/10.1111/j.15591816.1986.tb01138.x>
- Dietz, P., & Martell, D. A. (2010). Commentary: Approaching and stalking public figures—A prerequisite to attack. *Journal of the American Academy of Psychiatry and the Law Online*, 38, 341–348.
- Douglas, K. S., Ogloff, J. R., & Hart, S. D. (2003). Evaluation of a model of violence risk assessment among forensic psychiatric patients. *Psychiatric Services*, 54, 1372–1379. <https://doi.org/10.1176/appi.ps.54.10.1372>
- Dror, I. E. (2016). A hierarchy of expert performance. *Journal of Applied Research in Memory and Cognition*, 5, 121–127. <https://doi.org/10.1016/j.jarmac.2016.03.001>
- Dror, I. E., & Hampikian, G. (2011). Subjectivity and bias in forensic DNA mixture interpretation. *Science & Justice*, 51, 204–208. <https://doi.org/10.1016/j.scijus.2011.08.004>
- Einhorn, H. J. (1974). Expert judgment: Some necessary conditions and an example. *Journal of Applied Psychology*, 59, 562–571. <https://doi.org/10.1037/h0037164>
- Elstein, A. S., & Schwarz, A. (2002). Clinical problem solving and diagnostic decision making: Selective review of the cognitive literature. *British Medical Journal*, 324, 729–732. <https://doi.org/10.1136/bmj.324.7339.729>
- Ericsson, K. A. (2008). Deliberate practice and acquisition of expert performance: A general overview. *Academic Emergency Medicine*, 15, 988–994. <https://doi.org/10.1111/j.15532712.2008.00227.x>
- Fahsing, I., & Ask, K. (2016). The making of an expert detective: The role of experience in English and Norwegian police officers' investigative decision-making. *Psychology, Crime & Law*, 22, 203–223. <https://doi.org/10.1080/1068316X.2015.1077249>
- Fein, R. A., & Vossekuil, B. (1998). *Protective intelligence and threat assessment investigations: A guide for state and local law enforcement officials*. Washington, DC: US Department of Justice, Office of Justice Programs, National Institute of Justice.
- Feldman, T., & Johnson, P. (1996). Workplace violence: A new form of lethal aggression. In H. V. Hall (Ed.), *Lethal violence 2000: A sourcebook on fetal domestic, acquaintance and stranger aggression* (pp. 311–338). Kamuela, HI: Pacific Institute for the Study of Conflict and Aggression.
- Guy, L. S., Packer, I. K., & Warnken, W. (2012). Assessing risk of violence using structured professional judgment guidelines. *Journal of Forensic Psychology Practice*, 12, 270–283. <https://doi.org/10.1080/15228932.2012.674471>
- Hoffmann, J., Meloy, J. R., Guldemann, A., & Ermer, A. (2011). Attacks on German public figures, 1968–2004: Warning behaviours, potentially lethal and non-lethal acts, psychiatric status, and motivations. *Behavioral Sciences & the Law*, 29, 155–179. <https://doi.org/10.1002/bsl.979>
- James, D. V., MacKenzie, R. D., & Farnham, F. R. (2014). *Communications Threat Assessment Protocol*. London: Theseus LLP.
- Joseph, G. M., & Patel, V. L. (1990). Domain knowledge and hypothesis generation in diagnostic reasoning. *Medical Decision Making*, 10, 31–46. <https://doi.org/10.1177/0272989X9001000107>
- Klein, G. (2008). Naturalistic decision making. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 50, 456–460. <https://doi.org/10.1518/001872008X288385>
- Kraut, R. E., & Poe, D. B. (1980). Behavioral roots of person perception: The deception judgments of customs inspectors and laymen. *Journal of Personality and Social Psychology*, 39, 784–798. <https://doi.org/10.1037/0022-3514.39.5.784>
- Majamaa, H., & Ytti, A. (1996). A survey of the conclusions drawn of similar footwear cases in various crime laboratories. *Forensic Science International*, 82, 109–120. [https://doi.org/10.1016/03790738\(96\)01972-X](https://doi.org/10.1016/03790738(96)01972-X)
- Masip, J., Herrero, C., Garrido, E., & Barba, A. (2011). Is the behaviour analysis interview just common sense? *Applied Cognitive Psychology*, 25, 593–604. <https://doi.org/10.1002/acp.1728>
- Meehl, P. E. (1954). *Clinical versus statistical prediction: A theoretical analysis and a review of the evidence*. Minneapolis: University of Minnesota Press. <https://doi.org/10.1037/11281-000>
- Meloy, J. R., Hart, S. D., & Hoffmann, J. (2014b). Threat assessment and threat management. In J. R. Meloy, & J. Hoffmann (Eds.), *International handbook of threat assessment* (pp. 3–17). New York, NY: Oxford University Press.

- Meloy, J. R., Hoffmann, J., Roshdi, K., Glaz-Ocik, J., & Guldemann, A. (2014a). Warning behaviours and their configurations across various domains of targeted violence. In J. R. Meloy, & J. Hoffmann (Eds.), *International handbook of threat assessment* (pp. 39–53). New York, NY: Oxford University Press.
- Meloy, J. R., White, S. G., & Hart, S. (2013). Workplace assessment of targeted violence risk: The development and reliability of the WAVR-21. *Journal of Forensic Sciences*, 58, 1353–1358. <https://doi.org/doi:10.1111/1556-4029.12196>
- Patel, V. L., & Groen, G. J. (1986). Knowledge based solution strategies in medical reasoning. *Cognitive Science*, 10, 91–116. https://doi.org/10.1207/s15516709cog1001_4
- Reyna, V. F., & Lloyd, F. J. (2006). Physician decision making and cardiac risk: Effects of knowledge, risk perception, risk tolerance, and fuzzy processing. *Journal of Experimental Psychology: Applied*, 12, 179–195. <https://doi.org/10.1037/1076-898x.12.3.179>
- Schmidt, H. G., & Rikers, R. M. (2007). How expertise develops in medicine: Knowledge encapsulation and illness script formation. *Medical Education*, 41, 1133–1139. <https://doi.org/10.1111/j.1365-2923.2007.02915.x>
- Shanteau, J., Weiss, D. J., Thomas, R. P., & Pounds, J. C. (2002). Performance-based assessment of expertise: How to decide if someone is an expert or not. *European Journal of Operational Research*, 136, 253–263. [https://doi.org/10.1016/S0377-2217\(01\)00113-8](https://doi.org/10.1016/S0377-2217(01)00113-8)
- Skeem, J. L., & Monahan, J. (2011). Current directions in violence risk assessment. *Current Directions in Psychological Science*, 20, 38–42. <https://doi.org/10.1177/0963721410397271>
- Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2004). Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk Analysis*, 24, 311–322. <https://doi.org/10.1111/j.0272-4332.2004.00433.x>
- Slovic, P., & Weber, E. U. (2002, April). *Perception of risk posed by extreme events*. Paper prepared for discussion at the conference Risk Management Strategies in an Uncertain World, New York.
- Stolper, E., Van de Wiel, M., Van Royen, P., Van Bokhoven, M., Van der Weijden, T., & Dinant, G. J. (2011). Gut feelings as a third track in general practitioners' diagnostic reasoning. *Journal of General Internal Medicine*, 26, 197–203. <https://doi.org/10.1007/s11606-0101524-5>
- Ulery, B. T., Hicklin, R. A., Buscaglia, J., & Roberts, M. A. (2012). Repeatability and reproducibility of decisions by latent fingerprint examiners. *PloS One*, 7, e32800. <https://doi.org/10.1371/journal.pone.0032800>
- Vossekuil, B., Fein, R. A., & Berglund, J. M. (2015). Threat assessment: Assessing the risk of targeted violence. *Journal of Threat Assessment and Management*, 2, 243. <https://doi.org/10.1037/tam0000055>
- Weber, E. U. (2001). Decision and choice: Risk, empirical studies. In N. J. Smelser, & B. Baltes (Eds.), *International encyclopedia of the social and behavioral sciences* (pp. 13347–13351). Amsterdam, NL: Elsevier. <https://doi.org/10.1016/b0-08-043076-7/00634-3>
- White, S. G., & Meloy, J. R. (2010). *The WAVR-21: A structured professional guide for the workplace assessment of violence risk*. San Diego: Specialized Training Services.

How to cite this article: Geurts R, Granhag PA, Ask K, Vrij A. Assessing threats of violence: Professional skill or common sense?. *J Investig Psychol Offender Profil*. 2017. <https://doi.org/10.1002/jip.1486>

APPENDIX A

"The numbers in parentheses indicate the specific pieces of information that were extracted for risk assessment. The numbers correspond with the numbers on the horizontal axes in Figure 1."

A.1 | Case "Terry"

After a 1-year relationship, Rebecca (29 years old) decided to break up with her boyfriend Terry (38 years old). Terry has been very bitter about this sudden ending. He felt betrayed and expected that Rebecca would change her mind and come back to him. One month ago, when Rebecca came by his house to pick up her belongings, Terry told her that she better think twice about the breakup if her life is worth something to her (14). Rebecca went to the police and reported that she has been threatened by her ex-boyfriend. So far, Rebecca has avoided all contact with Terry (12). She has received a new telephone number and moved to another neighbourhood (13). Rebecca has a new boyfriend, and Terry recently found out about this (15).

The police took up the case and gathered some more information. It appeared that when Terry was a child, he often bullied other children and ruined their property (1). Terry was expelled from school at the age of 16 (2) and started working in a logistics company. At the age of 19, he served 5 years in prison for bank robbery (3). Back then, Terry stated that he did not feel bad for the bank employees who were present during the robbery, as it was not their money he had taken (4). Terry left his latest job as a construction worker because he could not get along with his boss (8). He is now thinking of setting up his own protein drink business (9). Terry collects exotic reptiles at home, such as lizards and chameleons (10). His back, chest, and arms are covered with tattoos of different types of reptiles (11). Furthermore, Terry has had many short-term relationships with women (5). He has four children with three of his ex-girlfriends. None of the children are Rebecca's (6). When Terry goes out with friends, he sometimes uses drugs, such as XTC or speed (7).

A.2 | Case "Marc"

Marc (24 years old) studies chemistry at the university and is in his final year. He has always been an excellent student (1). Two years ago, Marc read an article claiming that the pharmaceutical industry is contaminated by a few influential companies with malevolent intent. The article triggered Marc's interest, even though he had never used substances or medication other than homeopathic cures (2). Since then, Marc has delved into the topic (10) and is more and more convinced that the pharmaceutical industry is a corrupt business (11). Marc believes that the government should take responsibility by ending collaboration with big pharmaceuticals companies. Marc has written several letters to the Minister of Health and Social Affairs. After all the hours he has spent helping the Minister to make the right decision, Marc is highly frustrated that the Minister has not replied (12). One week ago, during a late evening round, a security guard found Marc in one of the university labs mixing various powders and liquids (13). When the guard asked him what he was doing, Marc answered, "If the Minister does not want to listen to reason, I will show him how poisonous their medication can be" (14). The security guard informed the university about this incident and Marc was temporarily suspended (15).

The university consulted an expert to investigate the case. This expert discovered that Marc's most recent letters to the Minister were accompanied by pictures and videotaped messages (16), in which he outlined his case against the pharmaceutical industry (17). In one video, Marc made a presentation for the National Pharmaceutical Association (NPA; 18). The NPA will have their annual board meeting 1 month from now (19). During this meeting, they will discuss new medicines and treatments. The meeting will take place 120 km from the city Marc lives in (20). The Minister will attend this meeting (21). Further information from Marc's acquaintances reveals that Marc was brought up by his grandparents (5), as his parents could not take care of him (6). Marc's clothing style is described by others as "gothic" (8) and he likes to listen to heavy metal bands such as *Led Zeppelin* (9). Marc never had many friends (3) and prefers to spend time alone (4). Yet, people described him as a friendly and good hearted guy (7).

A.3 | Case "Frank"

Frank (52 years old) works as an administrator for a big law firm. He started in this job 30 years ago when he was a law student. Back then, he hoped to eventually work there as lawyer. Much to his disappointment, he has never been promoted (8). Nevertheless, Frank never resigned from his job (9) and often tells outsiders about his company and the high-profile cases they handle (10). Three weeks ago, Frank's manager called him into his office. As Frank's 30 year anniversary at the firm was coming up (11), Frank expected that they would talk about the arrangements for the party (12). Instead, the manager discussed the upcoming reorganisation of the company and forced redundancies. The manager told Frank that his position with the firm is uncertain (13). Frank has called in sick every day since then (14). Yesterday, a note was taped on the entrance of the firm stating "I hate you all and one day soon you will hate me too" (18).

The firm consulted their internal Security & Integrity Team (SIT) and mentioned Frank as a subject of concern. SIT gathered the following additional information. Frank has type 1 diabetes and therefore needs daily insulin doses (6). Furthermore, Frank's acquaintances state that he is often angry (1) and feels that he is being wronged (2). From

Frank's perspective, people are either for or against him (3). Frank and his wife divorced 8 years ago (4), and he has suffered from depressive episodes ever since (5). Frank and his ex-wife bought an expensive house together. After the divorce, Frank was able to keep the house, but a large share of his monthly income goes to the mortgage payment (7). Frank normally joins a running group twice a week (15); however, he has not shown up in the last 3 weeks (16). Once per year, Frank travels abroad to attend a 3-day science fiction event (17).

Although Frank's case is under examination, the management of the law firm has called for an internal meeting with the entire staff (19). The new management arrangements will be explained and the exact number of redundancies will be announced. The meeting will be held 4 days from now (20). Frank has been invited to attend (21).